(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-342246
(P2004-342246A)
(43)公開日　平成16年12月2日(2004.12.2)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G11B 20/10	G11B 20/10	H	5B017
G06F 12/14	G06F 12/14	320B	5D044
G11B 20/12	G06F 12/14	320E	5D110
G11B 27/00	G06F 12/14	320F	5J104
H04L 9/08	G11B 20/12		

審査請求 未請求　請求項の数 28　OL　（全 46 頁）　最終頁に続く

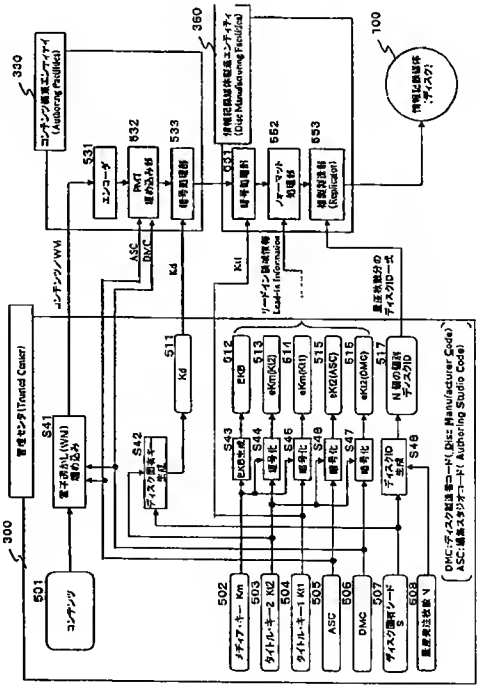
(21)出願番号　特願2003-138551(P2003-138551)
(22)出願日　平成15年5月16日(2003.5.16)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　木谷　聡
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】情報記録媒体に格納される暗号化コンテンツの不正利用の防止、不正複製についての情報漏えいルート解析を可能とした構成を提供する。
【解決手段】コンテンツ編集エンティテイが、記録シード（ＲＥＣ　ＳＥＥＤ）を生成し、管理センタから受領する鍵情報、および鍵生成情報（第２シード）に基づいて第２ブロックキーＫｂ２を生成し、第２ブロックキーＫｂ２に基づくコンテンツ暗号化を実行する。情報記録媒体製造エンティテイが、物理インデックスを生成し、管理センタから受領する鍵情報、および鍵生成情報（第１シード）に基づいてブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づく第２シードの暗号化を実行し、これらの情報および各エンティテイのコード情報を情報記録媒体に格納する。
【選択図】　図１８



【特許請求の範囲】
【請求項１】
情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理装置であり、
情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段と、
前記暗号処理手段において復号されたコンテンツの再生制御処理を実行する再生制御手段を有し、
前記暗号処理手段は、
前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力し、
前記再生制御手段は、前記暗号処理手段から受領する前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティテイに対応して設定された暗号化エンティテイコードの復号処理を実行して第１のエンティテイコードを算出するとともに、復号コンテンツ内に格納された第２のエンティテイコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする情報処理装置。
【請求項２】
前記再生制御手段は、
前記鍵情報を適用した前記暗号化エンティテイコードの復号処理を実行して、第１の編集スタジオコードと第１の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードを取得し、編集スタジオコードおよび情報記録媒体製造者コード各々について、第１コードと第２コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）に含まれる編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）であることを特徴とする請求項２に記載の情報処理装置。
【請求項４】
前記再生制御手段は、
前記鍵情報を適用した前記暗号化エンティテイコードの復号処理を実行して、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得し、
編集スタジオコード（ＡＳＣ）および情報記録媒体製造者コード（ＤＭＣ）各々について、第１コードと第２コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記暗号処理手段は、
前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成を有することを特徴とする請求項１

に記載の情報処理装置。
【請求項６】
前記暗号処理手段は、
前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしてのＥＫＢ（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行する構成を有することを特徴とする請求項１に記載の情報処理装置。
【請求項７】
前記暗号処理手段は、
前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、前記再生制御手段に出力し、
前記再生制御手段は、
前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第１のエンティティコードを算出する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項８】
前記暗号処理手段は、
前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体ＩＤを読み取り、該情報記録媒体ＩＤの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。
【請求項９】
前記暗号処理手段は、
前記情報記録媒体ＩＤに付加された電子署名の検証処理を実行し、該情報記録媒体ＩＤの改竄のないことの確認を条件として、前記情報記録媒体ＩＤの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする請求項８に記載の情報処理装置。
【請求項１０】
暗号化コンテンツを格納した情報記録媒体であり、
コンテンツの利用ライセンスを持つユーザデバイスに格納されたデバイスキーによってのみ復号処理可能な暗号化キーブロックとしてのＥＫＢ（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）と、
前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードの暗号化情報としての暗号化エンティティコードと、
前記製造ルートのエンティティに対応して設定された第２のコード情報を含む暗号化コンテンツと、
を格納した構成を有することを特徴とする情報記録媒体。
【請求項１１】
前記暗号化エンティティコードは、前記ＥＫＢの復号によって取得可能な鍵を適用した処理によって算出可能なコードであることを特徴とする請求項１０に記載の情報記録媒体。
【請求項１２】
前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードは、編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）を含み、
前記暗号化コンテンツにも、編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）を含む構成であることを特徴とする請求項１０に記載の情報記録媒

体。
【請求項１３】
前記暗号化コンテンツに含まれる前記第２のコード情報は、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を含むプログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）であることを特徴とする請求項１０に記載の情報記録媒体。
【請求項１４】
前記暗号化コンテンツに含まれる前記第２のコード情報は、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を含む電子透かし情報であることを特徴とする請求項１０に記載の情報記録媒体。
【請求項１５】
前記情報記録媒体は、
暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードと、
前記第１シードに基づいて生成される第１ブロックキーＫｂ１に基づいて暗号化された鍵生成情報としての暗号化第２シードと、
前記第２シードに基づいて生成される第２ブロックキーＫｂ２に基づいて暗号化された暗号化コンテンツと、
を格納した構成であることを特徴とする請求項１０に記載の情報記録媒体。
【請求項１６】
前記情報記録媒体は、さらに、
前記情報記録媒体の製造ルートのエンティテイである編集スタジオ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）と情報記録媒体製造者（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）各々が生成した鍵生成情報を含み、
前記情報記録媒体製造者の鍵生成情報と前記第１シードとに基づいて前記第１ブロックキーＫｂ１が生成され、
前記編集スタジオの鍵生成情報と前記第２シードとに基づいて前記第２ブロックキーＫｂ２が生成される構成であることを特徴とする請求項１５に記載の情報記録媒体。
【請求項１７】
コンテンツを格納した情報記録媒体の製造および利用管理を実行するコンテンツ管理システムであり、
コンテンツ管理エンティテイとしての管理センタが、コンテンツ編集を実行するコンテンツ編集エンティテイと、コンテンツを格納した情報記録媒体の製造を実行する情報記録媒体製造エンティテイとに対応するコード情報として編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）を生成し、
前記コンテンツ編集エンティテイは、前記編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を前記管理センタから受領して暗号化コンテンツ中に埋め込み、
前記情報記録媒体製造エンティテイは、前記編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を暗号化した暗号化コードを前記管理センタから受領して該暗号化コードを情報記録媒体に格納する処理を実行する構成を有することを特徴とするコンテンツ管理システム。
【請求項１８】
前記コンテンツ編集エンティテイは、
鍵生成情報としての記録シード（ＲＥＣ　ＳＥＥＤ）を生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第２シード）とに基づいて第２ブロックキーＫｂ２を生成し、該第２ブロックキーＫｂ２に基づくコンテンツ暗号化を実行し、
前記情報記録媒体製造エンティテイは、
鍵生成情報としての物理インデックスを生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第１シード）に基づいてブロックキーＫｂ１を生成し、該第１ブロック

キーＫｂ１に基づく前記第２シードの暗号化を実行する構成であることを特徴とする請求項１７に記載のコンテンツ管理システム。

【請求項１９】

情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理方法であり、

前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力する暗号処理ステップと、

前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第１のエンティティコードを算出するとともに、復号コンテンツ内に格納された第２のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、

を有することを特徴とする情報処理方法。

【請求項２０】

前記再生制御ステップは、

前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、第１の編集スタジオコードと第１の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードを取得するステップと、

編集スタジオコードおよび情報記録媒体製造者コード各々について、第１コードと第２コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、

を含むことを特徴とする請求項１９に記載の情報処理方法。

【請求項２１】

前記復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）に含まれる編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）であることを特徴とする請求項２０に記載の情報処理方法。

【請求項２２】

前記再生制御ステップは、

前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得するステップと、

編集スタジオコード（ＡＳＣ）および情報記録媒体製造者コード（ＤＭＣ）各々について、第１コードと第２コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、

を含むことを特徴とする請求項１９に記載の情報処理方法。

【請求項２３】

前記暗号処理ステップは、

前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップを含むことを特徴とする請求項１９に記載の情報処理方法。

【請求項２４】
前記暗号処理ステップは、
前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしてのＥＫＢ（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行するステップを含むことを特徴とする請求項１９に記載の情報処理方法。
【請求項２５】
前記暗号処理ステップは、
前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、
前記再生制御ステップは、
前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第１のエンティティコードを算出するステップを含むことを特徴とする請求項１９に記載の情報処理方法。
【請求項２６】
前記暗号処理ステップは、
前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体ＩＤを読み取り、該情報記録媒体ＩＤの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする請求項１９に記載の情報処理方法。
【請求項２７】
前記暗号処理ステップは、
前記情報記録媒体ＩＤに付加された電子署名の検証処理を実行し、該情報記録媒体ＩＤの改竄のないことの確認を条件として、前記情報記録媒体ＩＤの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする請求項２６に記載の情報処理方法。
【請求項２８】
情報記録媒体に格納された暗号化データの復号および再生制御を実行するコンピュータ・プログラムであり、
前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力する暗号処理ステップと、
前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第１のエンティティコードを算出するとともに、復号コンテンツ内に格納された第２のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、
を有することを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムに関する。詳細には、情報記録媒体を利用したデータ記録再生処理における不正なコンテンツ利用を防止する情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムに関する。
【０００２】

【従来の技術】
昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Ｃｏｎｔｅｎｔ）と呼ぶ）が、インターネット等のネットワークを介して、あるいはＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）、ＭＤ（Ｍｉｎｉ　Ｄｉｓｃ）等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）、ＣＤプレーヤ、ＤＶＤプレーヤ、ＭＤプレーヤ等の再生装置、あるいはゲーム機器等において再生され利用される。

【０００３】
音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

【０００４】
特に、近年においては、情報をデジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをＣＤ－Ｒ等にコピーした、いわゆる海賊版ディスクが大量に流通しているという問題がある。

【０００５】
特に、近年開発されたＤＶＤ等の大容量型記録媒体は、１枚の媒体に例えば映画１本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。

【０００６】
デジタル記録再生を行う記録装置やデジタル記録媒体によれば、画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通すると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

【０００７】
例えば、ＤＶＤプレーヤでは、ＣＳＳ（Ｃｏｎｔｅｎｔ　Ｓｃｒａｍｂｌｅ　Ｓｙｓｔｅｍ）が採用されている。ＣＳＳでは、ＤＶＤ－ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いる鍵が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

【０００８】
一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するための鍵を有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、ＣＳＳの構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、デジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。

【０００９】
しかしながら、ＤＶＤ－ＲＯＭで採用されているＣＳＳは、ユーザによるデータの書き込

みが不可能な記録媒体を対象としており、ユーザによるデータの書き込みが可能な記録媒体への適用については考慮されていない。

【００１０】

即ち、データの書き込みが可能な記録媒体に記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【００１１】

さらに、ＣＳＳの暗号を破るソフトウェアプログラム、例えばＤｅＣＳＳソフトウェアがインターネット上で配布されており、このプログラムを適用することで、ＤＶＤ Ｖｉｄｅｏの暗号を解いて平文の状態で記録型ＤＶＤへ書き込むことが可能になっている。ＤｅＣＳＳが出現した背景は、本来解読防止のための実装時の隠蔽対応が義務付けられているはずのＣＳＳ復号用の鍵データを何の対処もしないまま設計されたＤＶＤプレーヤー・ソフトウェアがリバースエンジニアされて鍵データが解読されたことであり、解読された鍵データから連鎖的にＣＳＳアルゴリズム全体が解読されたという経緯である。

【００１２】

鍵データを含む著作権保護技術実行プログラムをＰＣ上で実行されるアプリケーションプログラムへ実装する際には、著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的であるが、対タンパー性の強度を示す指標は無く、そのためどれほどリバースエンジニアリングへの対応を行うかは個々のインプレメンターの判断や実力に委ねられているのが実情であり、ＣＳＳの場合には結果として破られてしまい、不正なコピーコンテンツの氾濫を招く結果となっている。

【００１３】

ＣＳＳ以外にも、ＤＶＤ規格で採用されている著作権保護技術（コピーコントロール技術）として、ＣＰＰＭ（Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ ｆｏｒ Ｐｒｅｒｅｃｏｒｄｅｄ Ｍｅｄｉａ）とＣＰＲＭ（Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ ｆｏｒ Ｒｅｃｏｒｄａｂｌｅ Ｍｅｄｉａ）がある。ＣＰＰＭは、再生専用のメディア（Ｐｒｅｒｅｃｏｒｄｅｄ Ｍｅｄｉａ）用に開発されたコピーコントロール技術であり、ＣＰＲＭは、記録可能なメディア（Ｒｅｃｏｒｄａｂｌｅ Ｍｅｄｉａ）用に開発されたコピーコントロール技術である。これらは、メディア（例えばディスク）側にメディアキーブロックと呼ばれる鍵情報を格納し、一方、再生装置、ＰＣ等、デバイス側にデバイスキーを格納し、これらの鍵の組み合わせにより、コピーコントロールを行うものである。

【００１４】

しかし、このようなＣＰＲＭや、ＣＰＰＭにおいても、デバイスとしてのＰＣやメディアとしてのディスク内に格納された鍵情報の漏洩の危険性を解消するといった根本的な問題解決を図る技術についての提案はなく、ＣＰＲＭや、ＣＰＰＭにおいても、鍵の漏洩によってコピーコントロールシステムが崩壊する危険性を常に有しているのが現状である。

【００１５】

なお、コンテンツの不正利用を防止する技術として、本出願人は、例えば特許文献１および特許文献２において、記録媒体に格納するコンテンツのデータブロック毎に異なる鍵を適用した暗号処理技術を提案した。すなわち、データブロック毎の鍵生成情報としてシードを設定し、ブロック毎に設定したシードを暗号鍵の生成に適用する構成により、従来の１つの鍵のみによるコンテンツ暗号化を複雑化して、暗号アルゴリズムの解読困難性を高めたものである。

【００１６】

しかし、上述の構成において、データブロック毎の鍵生成情報としてシードは、記録媒体に格納された情報そのものを使用したものであり、前述のＣＳＳと同様の経緯で鍵データが解読され、解読された鍵データとデータブロック毎に異なるシードからブロックキーが導かれることによりコンテンツの漏洩を引き起こす懸念が皆無とはいえない。

【００１７】

また、コンテンツを格納したＣＤ、ＤＶＤ等の情報記録媒体を製造する場合、コンテンツ

編集者と、ディスク製造者とはそれぞれ別のエンティテイとして存在するのが通常であり、コンテンツ編集者において、あるいはディスク製造者の一方において適切な管理を実行しても不十分であり、双方のエンティテイにおいて適切な管理を行うことが必要となる。

【００１８】

しかし、現状においては、コンテンツを格納した情報記録媒体の製造ルートにおけるコンテンツ管理、鍵情報管理を総括的にかつ効率的に実行する適切な構成が実現されているとは言い難く、不正なコピー媒体が市場に流通した場合、その情報漏洩ルートを追跡することは困難となるというのが現状であった。特にコンテンツ編集者自身によるコンテンツの盗難行為やディスク製造者自身による盗難されたコンテンツの製造の結果として市場に流通する媒体は正規品との判別が困難であり、不正な媒体の市場への流通は一層深刻な状況となりつつある。

【００１９】

【特許文献１】

特許公開２００１－３５１３２４号公報

【特許文献２】

特許公開２００２－２３６６２２号公報

【００２０】

【発明が解決しようとする課題】

本発明は、上述の従来技術における問題点に鑑みてなされたものであり、ＤＶＤ、ＣＤ等の各種情報記録媒体に格納したコンテンツを再生装置、ＰＣ（パーソナルコンピュータ）等の情報処理装置において利用する構成において、記録媒体に格納するコンテンツの暗号化に適用する鍵情報の漏洩を困難とし、鍵解読、暗号アルゴリズムの解読の困難性を高めることを実現するとともに、不正に複製されたＤＶＤ、ＣＤ等の各種情報記録媒体が流通した場合において、その流通経路の効率的な追跡を可能とし、不正品の再生制限を可能とした情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００２１】

【課題を解決するための手段】

本発明の第１の側面は、

情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理装置であり、

情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段と、

前記暗号処理手段において復号されたコンテンツの再生制御処理を実行する再生制御手段を有し、

前記暗号処理手段は、

前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力し、

前記再生制御手段は、前記暗号処理手段から受領する前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティテイに対応して設定された暗号化エンティテイコードの復号処理を実行して第１のエンティテイコードを算出するとともに、復号コンテンツ内に格納された第２のエンティテイコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする情報処理装置にある。

【００２２】

さらに、本発明の情報処理装置の一実施態様において、前記再生制御手段は、前記鍵情報を適用した前記暗号化エンティテイコードの復号処理を実行して、第１の編集スタジオコードと第１の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードを取得し、編集スタジオコードおよび情報記録媒体製造者コード各々について、第１コードと第２コード間の照

合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする。

【００２３】

さらに、本発明の情報処理装置の一実施態様において、前記復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）に含まれる編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）であることを特徴とする。

【００２４】

さらに、本発明の情報処理装置の一実施態様において、前記再生制御手段は、前記鍵情報を適用した前記暗号化エンティティコードの復号処理を実行して、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得し、編集スタジオコード（ＡＳＣ）および情報記録媒体製造者コード（ＤＭＣ）各々について、第１コードと第２コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する構成を有することを特徴とする。

【００２５】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成を有することを特徴とする。

【００２６】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしてのＥＫＢ（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行する構成を有することを特徴とする。

【００２７】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、前記再生制御手段に出力し、前記再生制御手段は、前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第１のエンティティコードを算出する構成であることを特徴とする。

【００２８】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体ＩＤを読み取り、該情報記録媒体ＩＤの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【００２９】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記情報記録媒体ＩＤに付加された電子署名の検証処理を実行し、該情報記録媒体ＩＤの改竄のないことの確認を条件として、前記情報記録媒体ＩＤの要素としてのディスク固有シードを取

得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行する構成であることを特徴とする。

【００３０】

さらに、本発明の第２の側面は、

暗号化コンテンツを格納した情報記録媒体であり、

コンテンツの利用ライセンスを持つユーザデバイスに格納されたデバイスキーによってのみ復号処理可能な暗号化キーブロックとしてのＥＫＢ（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）と、

前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードの暗号化情報としての暗号化エンティティコードと、

前記製造ルートのエンティティに対応して設定された第２のコード情報を含む暗号化コンテンツと、

を格納した構成を有することを特徴とする情報記録媒体にある。

【００３１】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化エンティティコードは、前記ＥＫＢの復号によって取得可能な鍵を適用した処理によって算出可能なコードであることを特徴とする。

【００３２】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体の製造ルートのエンティティに対応して設定されたコードは、編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）を含み、前記暗号化コンテンツにも、編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）を含む構成であることを特徴とする。

【００３３】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化コンテンツに含まれる前記第２のコード情報は、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を含むプログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）であることを特徴とする。

【００３４】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化コンテンツに含まれる前記第２のコード情報は、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を含む電子透かし情報であることを特徴とする。

【００３５】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードと、前記第１シードに基づいて生成される第１ブロックキーＫｂ１に基づいて暗号化された鍵生成情報としての暗号化第２シードと、前記第２シードに基づいて生成される第２ブロックキーＫｂ２に基づいて暗号化された暗号化コンテンツと、を格納した構成であることを特徴とする。

【００３６】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、さらに、前記情報記録媒体の製造ルートのエンティティである編集スタジオ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）と情報記録媒体製造者（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）各々が生成した鍵生成情報を含み、前記情報記録媒体製造者の鍵生成情報と前記第１シードとに基づいて前記第１ブロックキーＫｂ１が生成され、前記編集スタジオの鍵生成情報と前記第２シードとに基づいて前記第２ブロックキーＫｂ２が生成される構成であることを特徴とする。

【００３７】

さらに、本発明の第３の側面は、
コンテンツを格納した情報記録媒体の製造および利用管理を実行するコンテンツ管理システムであり、
コンテンツ管理エンティテイとしての管理センタが、コンテンツ編集を実行するコンテンツ編集エンティテイと、コンテンツを格納した情報記録媒体の製造を実行する情報記録媒体製造エンティテイとに対応するコード情報として編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）を生成し、
前記コンテンツ編集エンティテイは、前記編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を前記管理センタから受領して暗号化コンテンツ中に埋め込み、
前記情報記録媒体製造エンティテイは、前記編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を暗号化した暗号化コードを前記管理センタから受領して該暗号化コードを情報記録媒体に格納する処理を実行する構成を有することを特徴とするコンテンツ管理システムにある。

【００３８】

さらに、本発明のコンテンツ管理システムの一実施態様において、前記コンテンツ編集エンティテイは、鍵生成情報としての記録シード（ＲＥＣ　ＳＥＥＤ）を生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第２シード）とに基づいて第２ブロックキーＫｂ２を生成し、該第２ブロックキーＫｂ２に基づくコンテンツ暗号化を実行し、前記情報記録媒体製造エンティテイは、鍵生成情報としての物理インデックスを生成し、前記管理センタから受領する鍵情報、および鍵生成情報（第１シード）に基づいてブロックキーＫｂ１を生成し、該第１ブロックキーＫｂ１に基づく前記第２シードの暗号化を実行する構成であることを特徴とする。

【００３９】

さらに、本発明の第４の側面は、
情報記録媒体に格納された暗号化データの復号および再生制御を実行する情報処理方法であり、
前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵情報を生成して、前記再生制御手段に出力する暗号処理ステップと、
前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティテイに対応して設定された暗号化エンティテイコードの復号処理を実行して第１のエンティテイコードを算出するとともに、復号コンテンツ内に格納された第２のエンティテイコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、
を有することを特徴とする情報処理方法にある。

【００４０】

さらに、本発明の情報処理方法の一実施態様において、前記再生制御ステップは、前記鍵情報を適用した前記暗号化エンティテイコードの復号処理を実行して、第１の編集スタジオコードと第１の情報記録媒体製造者コードを取得するとともに、復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードを取得するステップと、編集スタジオコードおよび情報記録媒体製造者コード各々について、第１コードと第２コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、を含むことを特徴とする。

【００４１】

さらに、本発明の情報処理方法の一実施態様において、前記復号コンテンツ内に格納された第２の編集スタジオコードと第２の情報記録媒体製造者コードは、復号コンテンツ内に格納されたプログラムマップテーブル（ＰＭＴ：Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）に含まれる編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）と情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄ

ｅ）であることを特徴とする。

【００４２】

さらに、本発明の情報処理方法の一実施態様において、前記再生制御ステップは、前記鍵情報を適用した前記暗号化エンティテイコードの復号処理を実行して、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得するとともに、復号コンテンツ内に格納された電子透かし情報から、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を取得するステップと、編集スタジオコード（ＡＳＣ）および情報記録媒体製造者コード（ＤＭＣ）各々について、第１コードと第２コード間の照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行するステップと、を含むことを特徴とする。

【００４３】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体に格納された暗号化コンテンツを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップを含むことを特徴とする。

【００４４】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報処理装置に格納されたデバイスキーに基づく、前記情報記録媒体に格納された暗号化キーブロックとしてのＥＫＢ（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）の復号により取得する鍵を適用して、前記情報処理装置に格納された暗号化コンテンツの復号、および、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行するステップを含むことを特徴とする。

【００４５】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行し、コンテンツまたはメディアに対応して設定されたタイトルキーを取得し、前記再生制御ステップは、前記タイトルキーを適用して前記情報記録媒体に格納された情報記録媒体製造ルートのエンティテイに対応して設定された暗号化エンティテイコードの復号処理を実行して第１のエンティテイコードを算出するステップを含むことを特徴とする。

【００４６】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体に格納された情報記録媒体固有の識別子としての情報記録媒体ＩＤを読み取り、該情報記録媒体ＩＤの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする。

【００４７】

さらに、本発明の情報処理方法の一実施態様において、前記暗号処理ステップは、前記情報記録媒体ＩＤに付加された電子署名の検証処理を実行し、該情報記録媒体ＩＤの改竄のないことの確認を条件として、前記情報記録媒体ＩＤの要素としてのディスク固有シードを取得し、該ディスク固有シードを適用して生成する鍵を用いて、前記情報処理装置に格納された暗号化コンテンツの復号処理を実行するステップを含むことを特徴とする。

【００４８】

さらに、本発明の第５の側面は、

情報記録媒体に格納された暗号化データの復号および再生制御を実行するコンピュータ・プログラムであり、

前記情報記録媒体に格納された暗号化コンテンツの復号処理を実行して復号コンテンツを生成するとともに、前記情報記録媒体に格納された暗号化鍵情報の復号処理を実行して鍵

情報を生成して、前記再生制御手段に出力する暗号処理ステップと、
前記鍵情報を適用して、前記情報記録媒体に格納された情報記録媒体製造ルートのエンティティに対応して設定された暗号化エンティティコードの復号処理を実行して第１のエンティティコードを算出するとともに、復号コンテンツ内に格納された第２のエンティティコードとの照合処理を実行し、該照合が不成立である場合、コンテンツ再生の停止処理を実行する再生制御ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

【００４９】

【作用】

本発明においては、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

【００５０】

さらに、本発明の構成によれば、情報記録媒体に格納されたコンテンツは、シード情報（シード１）およびシード情報（シード２）によって生成されるブロック鍵Ｋｂ１，Ｋｂ２で暗号化され、シード情報（シード２）は、シード情報（シード１）を用いて生成される鍵、すなわちブロックキーＫｂ１によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード２）の解析、シード情報（シード２）を適用して生成するブロックキーＫｂ２の解析、ブロックキーＫｂ２によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

【００５１】

さらに、本発明の構成によれば、コンテンツ編集エンティティが、鍵生成情報としての記録シード（ＲＥＣ　ＳＥＥＤ）を生成し、管理センタから受領する鍵情報、および鍵生成情報（第２シード）とに基づいて第２ブロックキーＫｂ２を生成し、第２ブロックキーＫｂ２に基づくコンテンツ暗号化を実行し、情報記録媒体製造エンティティが、鍵生成情報としての物理インデックスを生成し、管理センタから受領する鍵情報、および鍵生成情報（第１シード）に基づいてブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づく第２シードの暗号化を実行する構成とし、さらに、各エンティティのコード情報を情報記録媒体に格納する構成としたので、管理センタによって管理されたコンテンツ編集エンティティおよび情報記録媒体製造エンティティのみが正規な暗号化コンテンツを編集し、情報記録媒体を製造することが可能となり、情報記録媒体が不正に複製された場合には、コード検出による情報漏洩ルートの解析が可能となる。

【００５２】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＤＶＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００５３】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００５４】

【発明の実施の形態】
以下、本発明の情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラムの詳細について説明する。
【００５５】
［記録媒体上のデータ記録構成および製造プロセス概要］
まず、本発明に係る情報記録媒体に格納されるデータ構成および製造プロセス概要について説明する。情報記録媒体に格納された暗号化データは、データ記録再生装置や、ＰＣ（パーソナルコンピュータ）において読み取られ、復号、再生される。
【００５６】
本発明の情報記録媒体に格納されるデータについて、図１を参照して説明する。図１には、ディスク状の情報記録媒体１００を例として示す。なお、本発明における情報記録媒体は、光、磁気、半導体、フラッシュメモリ等、様々な形体の情報記録媒体を含み、ディスク状のものに限定されるものではない。
【００５７】
図１に示すように、情報記録媒体１００には、ディスクＩＤ１０１、物理インデックス１０２、暗号化コンテンツ１０３、記録シード（ＲＥＣ　ＳＥＥＤ）１０４、暗号鍵情報１２０が格納される。暗号鍵情報１２０は、情報記録媒体１００のコンテンツ格納領域とは異なる特別のプログラムに基づいて読み取り可能なリードイン領域１１０に格納される。
【００５８】
暗号鍵情報１２０には、情報記録媒体１００に格納された暗号化コンテンツ１０３の復号、再生に必要な様々な鍵情報が含まれる。図１、図２を参照して、情報記録媒体に格納される情報の概要と、情報記録媒体の製造ルートについて説明する。
【００５９】
図２に示すように、情報記録媒体に格納するコンテンツは、コンテンツ編集エンティテイ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）３３０において編集され、その後、情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）３５０において、ユーザに提供される媒体としてのＣＤ、ＤＶＤ等が大量に複製（レプリカ）されて、情報記録媒体１００が製造され、ユーザに提供される。情報記録媒体１００はユーザの情報処理装置２００において再生される。
【００６０】
このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ（ＴＣ：Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ）３００である。管理センタ（ＴＣ：Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ）３００は、コンテンツ編集エンティテイ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）３３０、および情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）３５０に対して様々な管理情報を提供し、コンテンツ編集エンティテイ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）３３０、および情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）３５０は、管理センタ（ＴＣ：Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ）３００から受領した管理情報に基づいて、コンテンツの編集、暗号化、鍵情報の、生成、格納処理などを行う。また、管理センタ（ＴＣ：Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ）３００は、ユーザの情報処理装置に格納するデバイスキーの管理、提供も行う。これらの各情報の詳細については後述する。
【００６１】
図１に示す暗号鍵情報１２０には、情報記録媒体１００に格納された暗号化コンテンツ１０３の復号、再生に必要な様々な鍵情報が含まれる。暗号鍵情報１２０は、管理センタ３００が生成し、情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）３５０に提供される。情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）３５０は、管理センタ３００から提供される暗号鍵情報１２０を情報記録媒体１００のリードイン領域１１０に格納する。
【００６２】
暗号鍵情報１２０には、コンテンツ再生に必要となるメディアキーＫｍを暗号化して格納

した暗号鍵ブロックとしてのＥＫＢ１２１、コンテンツまたはメディアに対応して設定される第１タイトルキー（Ｋｔ１）をメディアキーＫｍで暗号化した暗号化第１タイトルキーｅＫｍ（Ｋｔ１）１２２、第２タイトルキー（Ｋｔ２）をメディアキーで暗号化した暗号化第２タイトルキーｅＫｍ（Ｋｔ２）１２３、コンテンツ編集エンティテイコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）を第２タイトルキーＫｔ２）で暗号化した暗号化ＡＳＣ：ｅＫｔ２（ＡＳＣ）１２４、情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）を第２タイトルキー（Ｋｔ２）で暗号化した暗号化ＤＭＣ：ｅＫｔ２（ＤＭＣ）１２５を含んでいる。

【００６３】

ＥＫＢ１２１は、有効化キーブロック（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）であり、有効なライセンスを持つユーザの情報処理装置に格納されたデバイスキーに基づく処理（復号）によってのみ、コンテンツの復号に必要なメディアキーを取得する鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式によって、ユーザデバイス（情報処理装置）のライセンスの有効性に基づく鍵取得を可能としたものであり、無効化（リボーク処理）されたユーザデバイスの鍵（メディアキー）取得を阻止可能としたものである。管理センタはＥＫＢに格納する鍵情報の変更により、特定のユーザデバイスに格納されたデバイスキーでは復号できない、すなわちコンテンツ復号に必要なメディアキーを取得できない構成を持つＥＫＢを生成することができる。

【００６４】

階層型木構造を適用した暗号鍵等の暗号データ提供処理について、図を参照して説明する。図３の最下段に示すナンバ０～１５が、例えばコンテンツ利用を行なう情報処理装置としてのユーザデバイスである。すなわち図３に示す階層ツリー（木）構造の各葉（リーフ：ｌｅａｆ）がそれぞれのデバイスに相当する。

【００６５】

各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図１に示す階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセット（デバイスキー（ＤＮＫ：Ｄｅｖｉｃｅ　Ｎｏｄｅ　Ｋｅｙ））をメモリに格納する。図３の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲ（ルートキー）から、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【００６６】

図３に示す木構造において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲをデバイスキーとして所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図３のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【００６７】

また、図３のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図３に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【００６８】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対し

ては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはＣＤ等の情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵を送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なうエンティティは、図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行可能となる。このようなグループは、図３のツリー中に複数存在する。

【００６９】

なお、ノードキー、リーフキーは、ある１つの管理センタ機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ機能を持つ管理システム、プロバイダ、決済機関等が実行可能である。

【００７０】

このツリー構造において、図３から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はデバイスキー（ＤＮＫ：Ｄｅｖｉｃｅ　Ｎｏｄｅ　Ｋｅｙ）として共通のキーＫ００、Ｋ０、ＫＲを含むデバイスキー（ＤＮＫ：Ｄｅｖｉｃｅ　Ｎｏｄｅ　Ｋｅｙ）を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００は、デバイス０，１，２，３に共通する保有キーとなる。また、新たなキーＫｎｅｗをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｎｅｗ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Ｋｎｅｗ）を解いて新たなキーＫｎｅｗを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【００７１】

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが例えば攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１，Ｋ００，Ｋ０，ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Ｇｅｎｅｒａｔｉｏｎ）：ｔの更新キーであることを示す。

【００７２】

更新キーの配布処理ついて説明する。キーの更新は、例えば、図４（Ａ）に示す有効化キーブロック（ＥＫＢ：Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、有効化キーブロック（ＥＫＢ）は、図４に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：Ｋｅｙ　Ｒｅｎｅｗａｌ　Ｂｌｏｃｋ）と呼ばれることもある。

【００７３】

図４（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図４の例は、図３に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布す

ることを目的として形成されたブロックデータである。図３から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【００７４】

図４（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図４（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。

【００７５】

一方、デバイスＫ００００．Ｋ０００１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイスＫ００００．Ｋ０００１は、図４（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図４（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００７６】

図３に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０，Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図４（Ｂ）の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００７７】

図４（Ｂ）に示すＥＫＢは、例えば特定のグループにおいてのみ取得可能なメディアキーＫｍを配布する場合に利用可能である。具体例として、図３に点線で示すグループ内のデバイス０，１，２，３にのみ利用可能なメディアキーＫｍを配布するとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たなメディアキーＫｍを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｍ）を図４（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【００７８】

すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのキー、例えばコンテンツの暗号化復号化に適用するメディアキーＫ（ｔ）ｍを得ることが可能になる。

【００７９】

図５に、ｔ時点でのキー、例えばコンテンツの暗号化復号化に適用するメディアキーＫ（ｔ）ｍをＥＫＢの処理によって取得する処理例を示す。ＥＫＢには、Ｋ（ｔ）００を用いてメディアキーＫ（ｔ）ｍを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｍ）と図４（Ｂ）に示すデータとが格納されているとする。ここでは、デバイス０の処理例を示す。

【００８０】

図５に示すように、デバイス０は、記録媒体に格納されている世代：ｔ時点のＥＫＢと自

分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて暗号化データＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｍ）を復号して更新メデイアキーＫ（ｔ）ｍを取得する。

【００８１】

また、別の例としてツリー構造のノードキーの更新は不必要で、時点ｔでのメデイアキーＫ（ｔ）ｍのみを必要な機器が得られればよいという場合もある。この場合、下記のような方式とすることができる。

【００８２】

いま、図３の例と同様にデバイス０，１，２にのみメデイアキーＫ（ｔ）ｍを送りたいとする。このときＥＫＢは、

バージョン（Ｖｅｒｓｉｏｎ）：ｔ

インデックス　暗号化キー

０００　　Ｅｎｃ（Ｋ０００，　Ｋ（ｔ）ｍ）

００１０　Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）ｍ）

となる。

【００８３】

デバイス０，１はＫ０００を用いて、またデバイス２はＫ００１０を用いて上記ＥＫＢのうちの１つの暗号文を復号することによりコンテンツ鍵を得ることができる。このようにすることにより、ノードキーの更新は行えないものの必要な機器にコンテンツ鍵を与える方法をより効率よく（すなわち、ＥＫＢに含まれる暗号文数を減らしてＥＫＢのサイズを小さくするとともに管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる）することができる。

【００８４】

図１に戻り、情報記録媒体１００に格納されるその他のデータの詳細について説明する。ディスクＩＤ１０１は、情報記録媒体固有の識別子としての情報記録媒体ＩＤである。管理センタ３００が生成して情報記録媒体製造エンティテイ３５０に渡す管理情報であり、ディスク１枚毎に異なるＩＤである。例えば、管理センタ３００はディスク１枚毎に異なるシード（Ｓ）を生成し、改竄検証用の電子署名（Ｓｉｇ）を付加したデータ（Ｓ，Ｓｉｇ）を管理センタが許容したディスク枚数分生成して情報記録媒体製造エンティテイ３５０に提供する。情報記録媒体製造エンティテイ３５０は、ディスク毎に異なるＩＤ情報（Ｓ，Ｓｉｇ）を情報記録媒体（ディスク）に格納する。

【００８５】

コンテンツ再生を実行するユーザの情報処理装置においては、情報記録媒体（ディスク）に格納されたＩＤ情報（Ｓ，Ｓｉｇ）を読み取り、署名検証処理によりＩＤの改竄のないことの確認を条件として、コンテンツ復号プロセスに移行する。なお、署名は公開鍵暗号方式に基づく署名、またはＭＡＣ等の共通鍵暗号方式による署名等の利用が可能である。公開鍵暗号方式に基づく署名を適用する場合は、管理センタ３００は、秘密鍵による署名生成を実行し、各ユーザの情報処理装置では、管理センタ３００の公開鍵による署名検証を実行する。共通鍵方式の場合は、管理センタ、ユーザデバイス双方において共通の署名用鍵を保有し、署名生成、検証処理を実行する。ユーザの情報処理装置（ユーザデバイス）における処理については後述する。

【００８６】

図１に示す情報記録媒体に格納される物理インデックス１０２は、情報記録媒体製造エンティテイ３５０が生成して、情報記録媒体に格納する。記録シード（ＲＥＣ　ＳＥＥＤ）１０４は、コンテンツ編集エンティテイ３３０が生成して、情報記録媒体製造エンティテイ３５０に渡されて情報記録媒体に格納する値である。

【００８７】

暗号化コンテンツ１０３は、暗号化コンテンツ中に、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）とを含むプログラムマップテーブルＰＭＴ（Ｐｒｏｇ

ｒａｍ　Ｍａｐ　Ｔａｂｌｅ）が格納される。ＰＭＴは編集スタジオコード（ＡＳＣ）と、情報記録媒体製造者コード（ＤＭＣ）を含む情報であり、コンテンツ編集エンティテイ３３０においてコンテンツに対して埋め込まれる。さらに、暗号化コンテンツ１０３には、電子透かし（ＷＭ：Ｗａｔｅｒ　Ｍａｒｋ）としても、コンテンツ編集エンティテイコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）、情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）が格納される。これらのコード埋め込みは、管理センタ３００において行われる。情報記録媒体に対する様々なデータ埋め込み処理の詳細なシーケンスについては、後述する。

【００８８】

情報記録媒体に格納される暗号化コンテンツは、例えばＭＰＥＧ－２システムで規定されている符号化データとしてのトランスポートストリーム（ＴＳ）として構成される。トランスポートストリームは、１本のストリームの中に複数のプログラムを構成することができ、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Ａｒｒｉｖａｌ　Ｔｉｍｅ　Ｓｔａｍｐ：着信時刻スタンプ）が設定されている。このタイムスタンプは、ＭＰＥＧ－２システムで規定されている仮想的なデコーダであるＴ－ＳＴＤ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ　Ｓｙｓｔｅｍ　Ｔａｒｇｅｔ　Ｄｅｃｏｄｅｒ）を破綻させないように符号化時に決定され、ストリームの再生時に、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御して、復号、再生を行う。

【００８９】

例えば、トランスポートストリームパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

【００９０】

図６を参照して、情報記録媒体に格納されるデータ記録構成および、記録データの復号再生処理の概要を説明する。情報記録媒体に格納されるデータは暗号化データであり、再生を行う場合には、復号処理を行うことが必要となる。図６（ａ）が情報記録媒体に格納されるデータ記録構成である。１８バイトの制御データ（Ｕｓｅｒ　Ｃｏｎｔｒｏｌ　Ｄａｔａ）と、２０４８バイトのユーザデータ（Ｕｓｅｒ　Ｄａｔａ）が１つのセクタデータとして構成され、例えば３セクタ分のデータが１つの暗号処理単位として規定される。なおここで説明するバイト数や、処理単位は１つの代表例であり、制御データ、ユーザデータのバイト数や、処理単位の設定は、様々な設定が可能である。

【００９１】

（ｂ）は、暗号処理単位である１ユニット（１ＡＵ：Ａｌｉｇｎｅｄ　Ｕｎｉｔ）の構成を示す。情報記録媒体に格納された暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Ａｌｉｇｎｅｄ　Ｕｎｉｔ）を抽出する。

【００９２】

暗号処理単位である１ユニット（１ＡＵ）には、（ｃ）暗号化構成に示すように、ブロックキーＫｂ１によって暗号化された領域、ブロックキーＫｂ２によって暗号化された領域が含まれる。ブロックキーＫｂ１とＫｂ２によって二重に暗号化された領域を含める構成としてもよい。ブロックキーを生成するためには、鍵生成情報としてのシード情報が必要となる。シード情報（シード１）はブロックキーＫｂ１を生成するための鍵生成情報であり、シード情報（シード２）はブロックキーＫｂ２を生成するための鍵生成情報である。これらは、制御データ領域、あるいはユーザデータ領域に格納される。図６（ｃ）に示すシード情報の格納態様、暗号化態様は一例であり、後段において、複数の構成例について説明する。

【００９３】

ユーザデータ領域に格納された暗号化コンテンツを復号するためには、情報記録媒体に格納されたシード情報を読み取って、シード情報に基づく鍵を生成することが必要となる。

【００９４】
図６（ｃ）に示すように、ブロックキーＫｂ１を生成するために必要となるシード情報（シード１）と、ブロックキーＫｂ２を生成するために必要となるシード情報（シード２）とを情報記録媒体上に格納するとともに、一方のシード情報（シード２）をシード情報（シード１）によって生成されるブロックキーＫｂ１によって暗号化して格納している。また、暗号化コンテンツ中に、電子透かし（ＷＭ：Ｗａｔｅｒ　Ｍａｒｋ）として、コンテンツ編集エンティティコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）、情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）が格納される。
【００９５】
このように、２つの異なる鍵を適用した暗号化処理を実行したデータを記録媒体に格納し、再生処理において２つの異なる鍵を適用した復号処理を行う。すなわち、所定の暗号処理単位毎に異なる鍵生成情報であるシード１、シード２を適用した暗号処理によりブロックキーＫｂ１，Ｋｂ２を生成して復号処理を実行する。
【００９６】
１処理単位毎の復号処理の後、復号されたトランスポートストリームパケットがＭＰＥＧ－２デコーダに入力されデコード処理が実行されてコンテンツ再生が行なわれる。１つの処理単位（３セクタ）には、例えば３２個のトランスポートストリーム（ＴＳ）パケットが含まれる。すなわち、３２×１９２＝６１４４バイトデータが１つの暗号化および復号処理単位とされる。なお、処理単位の設定は、様々な設定が可能である。
【００９７】
復号再生時には、各処理単位毎に２つのシード情報（シード１、シード２）を情報記録媒体から取得し、各シード情報に基づいて２つのブロックキーＫｂ１、Ｋｂ２を生成し、生成したブロックキーＫｂ１，Ｋｂ２を用いて復号処理がなされて、コンテンツ再生が行われる。
【００９８】
また、コンテンツの記録時には、復号再生処理と逆のプロセスが実行され、各処理単位毎に２つのシード情報（シード１、シード２）を設定し、各シード情報に基づいて２つのブロックキーＫｂ１、Ｋｂ２を生成し生成したブロックキーＫｂ１，Ｋｂ２を用いて暗号化処理がなされて、コンテンツ記録が行われる。
【００９９】
【０１００】
［情報処理装置構成］
図７は、上述した暗号化コンテンツ態様を持つコンテンツの記録再生処理を実行する情報処理装置２００の一実施例構成を示すブロック図である。情報処理装置２００は、入出力Ｉ／Ｆ（Ｉｎｔｅｒｆａｃｅ）２２０、ＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）コーデック２３０、Ａ／Ｄ，Ｄ／Ａコンバータ２４１を備えた入出力Ｉ／Ｆ（Ｉｎｔｅｒｆａｃｅ）２４０、暗号処理手段２５０、再生制御処理手段２５５、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２６０、ＣＰＵ（ＣｅｎｔｒａＩ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）２７０、メモリ２８０、記録媒体２９５のドライブ２９０、さらにトランスポートストリーム処理手段（ＴＳ処理手段）２９８を有し、これらはバス２１０によって相互に接続されている。
【０１０１】
入出力Ｉ／Ｆ２２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス２１０上に出力するとともに、バス２１０上のデジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック２３０は、バス２１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ２４０に出力するとともに、入出力Ｉ／Ｆ２４０から供給されるデジタル信号をＭＰＥＧエンコードしてバス２１０上に出力する。入出力Ｉ／Ｆ２４０は、Ａ／Ｄ，Ｄ／Ａコンバータ２４１を内蔵している。入出力Ｉ／Ｆ２４０は、外部から供給されるコンテンツとしてのア

ナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ２４１でＡ／Ｄ（Ａｎａｌｏｇ　ｔｏ　Ｄｉｇｉｔａｌ）変換することで、デジタル信号として、ＭＰＥＧコーデック２３０に出力するとともに、ＭＰＥＧコーデック２３０からのデジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ２４１でＤ／Ａ（Ｄｉｇｉｔａｌ　ｔｏ　Ａｎａｌｏｇ）変換することで、アナログ信号として、外部に出力する。

【０１０２】

暗号処理手段２５０は、例えば、１チップのＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）で構成され、バス２１０を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス２１０上に出力する構成を持つ。再生制御処理手段２５５は、コンテンツ再生において検証すべき各種処理を実行して、再生条件を満足しない場合には、コンテンツ再生の停止を行う。暗号処理手段２５０および再生制御処理手段２５５の処理の詳細については後述する。

【０１０３】

なお、暗号処理手段２５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。図においては、暗号処理手段２５０、再生制御処理手段２５５をそれぞれ個別のブロックとして示してあるが、これらはたとえばＣＰＵ２７０の制御の下に実行するプログラムに基づいて実行する処理とすることも可能である。

【０１０４】

ＲＯＭ２６０は、例えば、情報処理装置ごとに固有の、あるいは、複数の情報処理装置のグループごとに固有のデバイスキーや、相互認証時に必要とする認証キーを記憶している。デバイスキーは、例えば鍵配信ツリー構成に基づいて提供される暗号化鍵ブロック情報としてのＥＫＢ（Ｅｎａｂｌｉｎｇ　Ｋｅｙ　Ｂｌｏｃｋ）を復号してメディアキーを取得するために用いられる。すなわち、デバイスキーは、メディアキー生成情報として適用される。

【０１０５】

ＣＰＵ２７０は、メモリ２８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック２３０や暗号処理手段２５０等を制御する。メモリ２８０は、例えば、不揮発性メモリで、ＣＰＵ２７０が実行するプログラムや、ＣＰＵ２７０の動作上必要なデータを記憶する。メモリ２８０が不揮発性メモリの場合、デバイスキーを記憶することも可能であり、以降の実施例ではデバイスキーはメモリ２８０へ格納するとして説明をする。ドライブ２９０は、デジタルデータを記録再生可能な記録媒体２９５を駆動することにより、記録媒体２９５からデジタルデータを読み出し（再生し）、バス２１０上に出力するとともに、バス２１０を介して供給されるデジタルデータを、記録媒体２９５に供給して記録させる。

【０１０６】

記録媒体２９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはフラッシュＲＯＭ、ＭＲＡＭ、ＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、図１を参照して説明した各種データを格納した情報記録媒体である。本実施の形態では、ドライブ２９０に対して着脱可能な構成であるとする。但し、記録媒体２９５は、情報処理装置２００に内蔵する構成としてもよい。

【０１０７】

トランスポートストリーム処理手段（ＴＳ処理手段）２９８は、複数のコンテンツが多重化されたトランスポートストリームから特定のコンテンツに対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体２９５に格納するためのデータ処理を実行し、また、記録媒体２９５からの暗号化コンテンツの復号再生時には、トランスポートストリームの出現タイミング制御を行なう。

【０１０８】

トランスポートストリームには、前述したように、各トランスポートパケットの出現タイ

ミング情報としてのＡＴＳ（Ａｒｒｉｖａｌ　Ｔｉｍｅ　Ｓｔａｍｐ：着信時刻スタンプ）が設定されており、ＭＰＥＧ２デコーダによる復号時にＡＴＳによってタイミング制御を実行する。トランスポートストリーム処理手段（ＴＳ処理手段）２９８は、例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

【０１０９】

本発明の情報処理装置２００は、例えば上述のトランスポートストリームによって構成される暗号化コンテンツの記録再生を実行する。これらの処理の詳細については、後段で説明する。なお、図７に示す暗号処理手段２５０、ＴＳ処理手段２９８は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する１つのワンチップＬＳＩとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。さらには、ドライブ２９０、記録媒体２９５を除く全てのブロックをワンチップＬＳＩとして構成してもよく、また、これらの機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよく、これにより情報処理装置２００の改造によるセキュリティ機能の無効化に対するロバストネスを向上させることが出来る。

【０１１０】

［データ再生処理］

次に、記録媒体に格納された暗号化データの復号処理および再生制御処理について説明する。図８に示すように、情報処理装置２００におけるコンテンツ再生は、暗号処理手段２５０における暗号化コンテンツの復号処理と、再生制御手段２５５における再生制御処理の２つのステップを含む。

【０１１１】

情報記録媒体１００から各種の情報が読み取られ、暗号処理手段２５０における暗号化コンテンツの復号処理が実行され、復号コンテンツが再生制御手段２５５に渡され、再生条件判定処理が実行され、再生条件を満足する場合にのみコンテンツ再生が継続して実行され、再生条件を満足しない場合には、コンテンツ再生が停止される。

【０１１２】

まず、暗号処理手段２５０における暗号化コンテンツの復号処理の詳細について、図９以下を参照して説明する。

【０１１３】

コンテンツ復号プロセスでは、まず、暗号処理手段２５０は、メモリに格納しているデバイスキー４１０を読み出す。デバイスキー４１０は、コンテンツ利用に関するライセンスを受けた情報処理装置に格納された秘密キーである。

【０１１４】

次に、暗号処理手段２５０は、ステップＳ１１において、デバイスキー４１０を適用して情報記録媒体１００に格納されたメディアキー格納ＥＫＢの復号処理を実行して、メディアキーＫｍを取得する。

【０１１５】

次に、ステップＳ１２において、情報記録媒体１００に格納されたメディアキーＫｍにより暗号化された暗号化第２タイトルキーｅＫｍ（Ｋｔ２）を、ステップＳ１１におけるＥＫＢ処理で取得したメディアキーＫｍを用いて復号し、第２タイトルキーＫｔ２を取得する。第２タイトルキーＫｔ２は、再生制御処理手段２５５に出力される。

【０１１６】

ステップＳ１３において、情報記録媒体１００に格納されたメディアキーＫｍにより暗号化された暗号化第１タイトルキーｅＫｍ（Ｋｔ１）を、ステップＳ１１におけるＥＫＢ処理で取得したメディアキーＫｍを用いて復号し、第１タイトルキーＫｔ１を取得する。

【０１１７】

次にステップＳ１４で、情報記録媒体１００に格納されたディスクＩＤからディスク固有シード（Ｓ）を取得する。暗号処理手段２５０は、情報記録媒体１００に格納された識別情報としてのディスクＩＤ（Ｄｉｓｃ　ＩＤ）４０４を読み出して、ディスクＩＤ４０４の検証処理を実行する。ディスクＩＤは、管理センタ３００が生成したディスク１枚毎に異なるシードＳと改竄検証用の電子署名（Ｓｉｇ）を持つデータ（Ｓ，Ｓｉｇ）である。暗号処理手段２５０は、情報記録媒体１００に格納されたＩＤ情報（Ｓ，Ｓｉｇ）を読み取り、署名検証処理によりＩＤの改竄のないことを確認する。公開鍵暗号方式に基づく署名の場合は、管理センタ３００の公開鍵による署名検証を実行する。共通鍵方式の場合は、共通鍵により署名検証処理を実行する。署名検証処理によりＩＤの改竄のないことの確認を条件として、ステップＳ１４で、情報記録媒体１００に格納されたディスクＩＤからディスク固有シードＳを取得する。署名検証処理によりＩＤの改竄があると判定した場合は、コンテンツ復号処理は停止する。

【０１１８】

署名検証処理によりＩＤの改竄のないことの確認がなされると、次に、ステップＳ１５において、ディスク固有シードＳと、タイトルキーＫ２を用いて、ディスク固有キー（Ｄｉｓｃ　Ｕｎｉｑｕｅ　Ｋｅｙ）Ｋｄを生成する。ディスク固有キー（Ｄｉｓｃ　Ｕｎｉｑｕｅ　Ｋｅｙ）の具体的な生成方法としては、例えば、図１０（ａ）に示すように、ディスク固有シードＳを入力値とし、共通鍵暗号方式であるＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号を、タイトルキーＫ２を暗号鍵として実行する方法や、図１０（ｂ）に示すように、ＦＩＰＳ　１８０－１で定められているハッシュ関数ＳＨＡ－１に、タイトルキーＫ２とディスク固有シードＳとのビット連結により生成されるデータを入力し、その出力から必要なデータ長のみをディスク固有キー（Ｄｉｓｃ　Ｕｎｉｑｕｅ　Ｋｅｙ）として使用する方法などが適用できる。

【０１１９】

さらに、暗号処理手段２５０は、ステップＳ１３において生成した第１タイトルキーＫｔ１と、情報記録媒体１００から読み出した物理インデックス４０６とに基づいて、ステップＳ１６において、第１記録キー（ＲＥＣキー）Ｋ１を生成し、また、ステップＳ１５において生成したディスク固有キーＫｄと、情報記録媒体１００から読み出した記録シード（ＲＥＣ　ＳＥＥＤ）４０５とに基づいて、ステップＳ１７において、第２記録キー（ＲＥＣキー）Ｋ２を生成する。これらの各キーの生成処理においてもＡＥＳ暗号処理等、ハッシュ関数、縮約関数などが適宜使用される。

【０１２０】

記録キーＫ１、Ｋ２は、上述の再生処理プロセスにおいて使用することが必要となるが、コンテンツを情報記録媒体に記録する暗号処理においても適用される鍵、記録処理については後述する。

【０１２１】

ステップＳ１６、Ｓ１７において２つの記録キー（ＲＥＣキー）１，２を生成すると、次に、ステップＳ１８から、情報記録媒体１００に格納された暗号化コンテンツ４０７の読み出しおよび２つのブロックキーＫｂ１，Ｋｂ２による復号処理が開始される。

【０１２２】

ステップＳ１８において、情報記録媒体１００に格納された暗号化コンテンツ４０７から制御情報（ＵＣＤ：Ｕｓｅｒ　Ｃｏｎｔｒｏｌ　Ｄａｔａ）に含まれるシード情報（シード１）が取得され、ステップＳ１９において、シード情報（シード１）と、ステップＳ１６において生成した第１記録キーＫ１とに基づく暗号処理を実行してブロックキーＫｂ１を生成する。

【０１２３】

ステップＳ１９のブロックキーＫｂ１の生成処理以降に実行する処理について、図９とともに図１１を参照して説明する。

【０１２４】

図１１において、復号処理は、処理単位４２０を単位として実行される。この処理単位は

、先に図６を参照して説明した（ｂ）処理単位に相当する。すなわち、暗号処理単位である１ユニット（１ＡＵ：Ａｌｉｇｎｅｄ　Ｕｎｉｔ）である。情報記録媒体１００に格納された暗号化データの再生を実行する暗号処理手段２５０は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Ａｌｉｇｎｅｄ　Ｕｎｉｔ）を抽出する。

【０１２５】

処理単位４２０には、１８バイトの制御データ（ＵＣＤ：Ｕｓｅｒ　Ｃｏｎｔｒｏｌ　Ｄａｔａ）４２１と、６１４４バイトのユーザデータ（暗号化コンテンツを含む）が含まれる。６１４４バイトのユーザデータは、トランスポートストリームパケットの単位である１９２バイト毎に分割される。ユーザデータの先頭のＴＳパケット４２２と、後続の５９５２バイトのＴＳパケット群４２３を分離して説明する。この例では、シード情報（シード１）４３１が制御データ４２１に格納され、シード情報（シード２）４３２がユーザデータ内の先頭のＴＳパケット４２２内に暗号化されて格納された例である。

【０１２６】

なお、シード情報としての、シード１、シード２の格納態様には複数の態様があり、ここではその一例を示す。他の例については、後段で説明する。

【０１２７】

図１１において、図９の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【０１２８】

ステップＳ１９（図９、図１１）においては、情報記録媒体の制御データ内から読み出したシード情報（シード１）４３１をＡＥＳ暗号処理部に入力し、先のステップＳ１６において生成した記録キーＫ１を適用したＡＥＳ暗号処理を実行しブロックキーＫｂ１を生成する処理を実行する。なお、図１１においてＡＥＳ＿Ｇは、ＡＥＳ暗号処理を適用した鍵生成（Ｋｅｙ　Ｇｅｎｅｒａｔｉｏｎ）処理を示し、ＡＥＳ＿Ｄは、ＡＥＳ暗号処理を適用したデータ復号（Ｄｅｃｒｙｐｔｉｏｎ）処理を示している。

【０１２９】

ステップＳ２０（図９、図１１参照）では、ステップＳ１９において生成したブロックキーＫｂ１を適用したＡＥＳ復号処理を実行する。ステップＳ２０では、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭ＴＳパケット４２２の少なくともシード情報（シード２）を含むデータ領域がブロックキーＫｂ１を適用した暗号処理のなされたデータ部である。従って、このシード情報（シード２）を含むデータ領域を対象としてブロックキーＫｂ１を適用した復号処理を実行する。

【０１３０】

なお、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては後述する。

【０１３１】

先頭ＴＳパケット４２２には、他のユーザデータ部、すなわち、後続の５９５２バイトのＴＳパケット群４２３の復号処理に適用するブロックキーＫｂ２を算出するために必要となるシード情報（シード２）４３２が含まれている。すなわち、シード情報（シード２）４３２は、ブロックキーＫｂ１を適用した暗号処理がなされた暗号化データとして先頭ＴＳパケット４２２に記録されている。

【０１３２】

ステップＳ２０における、ブロックキーＫｂ１を適用した復号処理の結果として、復号ＴＳパケット４２４が算出され、その中からシード情報（シード２）を抽出する。

【０１３３】

図９のセレクタステップＳ２１は、ブロックキーＫｂ１を適用した復号処理の結果から、シード情報（シード２）をステップＳ２２のブロックキーＫｂ２生成ステップに出力し、ブロックキーＫｂ２で暗号化された暗号化データを復号ステップＳ２３に出力し、その他の復号データ（非暗号化データ）をセレクタステップＳ２４に出力することを示している

。

【０１３４】

ステップＳ２２（図９，図１１参照）では、ステップＳ２０におけるブロックキーＫｂ１を適用した復号処理の結果取得された復号ＴＳパケット４２４から抽出したシード情報（シード２）と、ステップＳ１７（図９参照）において生成した記録キーＫ２とに基づいて、ＡＥＳ暗号処理を実行し、ブロックキーＫｂ２を算出する。

【０１３５】

次に、ステップＳ２３において、ブロックキーＫｂ２を適用してユーザデータ部の暗号化部（ブロックキーＫｂ２で暗号化されたデータ領域４２３）を復号し、復号ＴＳパケット群４２５を生成する。

【０１３６】

復号ＴＳパケット群４２５、および復号ＴＳパケット４２６（＝ＴＳパケット４２４）は、セレクタステップＳ２４において結合されて、復号ＴＳパケットからなるコンテンツ４１２として再生制御処理手段２５５に入力される。

【０１３７】

再生制御処理手段２５５における再生制御処理について、図１２を参照して説明する。再生制御処理手段２５５は、暗号処理手段２５０から、第２タイトルキー（Ｋｔ２），４１１と、復号コンテンツ４１２を受領する。

【０１３８】

まず、再生制御処理手段２５５は、ステップＳ３１において、情報記録媒体１００に格納された暗号化ＡＳＣすなわち、第２タイトルキー（Ｋｔ２）で暗号化した編集スタジオコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）であるデータｅＫｔ２（ＡＳＣ）を読み出し、暗号処理手段２５０から受信した第２タイトルキー（Ｋｔ２）を適用して復号処理を実行し、編集スタジオコード（ＡＳＣ）を取得しメモリに格納する。

【０１３９】

さらに、再生制御処理手段２５５は、ステップＳ３２において、情報記録媒体１００に格納された暗号化ＤＭＣすなわち、第２タイトルキー（Ｋｔ２）で暗号化した情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）であるデータｅＫｔ２（ＤＭＣ）を読み出し、暗号処理手段２５０から受信した第２タイトルキー（Ｋｔ２）を適用して復号処理を実行し、情報記録媒体製造者コード（ＤＭＣ）を取得しメモリに格納する。

【０１４０】

再生制御処理手段２５５は、暗号処理手段２５０から受信した復号コンテンツ４１２から、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）とを含むプログラムマップテーブルＰＭＴ（Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）を検出する。ＰＭＴは編集スタジオコード（ＡＳＣ）と、情報記録媒体製造者コード（ＤＭＣ）を含む情報であり、コンテンツ編集エンティテイ３３０においてコンテンツに対して埋め込まれる。ステップＳ３３において編集スタジオコード（ＡＳＣ）検出、ステップＳ３４において情報記録媒体製造者コード（ＤＭＣ）検出を実行する。

【０１４１】

ステップＳ３５において、ＰＭＴから検出した編集スタジオコード（ＡＳＣ）と、ステップＳ３１で、暗号化編集スタジオコードｅＫｔ２（ＡＳＣ）の復号処理によって取得しメモリに格納した編集スタジオコード（ＡＳＣ）との比較処理を実行する。

【０１４２】

さらに、ステップＳ３６において、ＰＭＴから検出した情報記録媒体製造者コード（ＤＭＣ）と、ステップＳ３２で、暗号化情報記録媒体製造者コード（ＤＭＣ）ｅＫｔ２（ＤＭＣ）の復号処理によって取得しメモリに格納した情報記録媒体製造者コード（ＤＭＣ）との比較処理を実行する。

【０１４３】

さらに、ステップＳ３７において、コンテンツ４１２中から、編集スタジオコード（ＡＳ

Ｃ）と情報記録媒体製造者コード（ＤＭＣ）を含む電子透かしが規定時間内に検出され、電子透かし格納情報と、メモリ格納情報とが一致したか否かを判定する。再生制御処理手段２５５では、コンテンツの再生開始からタイマを設定し、予め定めた定時間内に編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を含む電子透かしが検出されたか否かを判定する。

【０１４４】

ステップＳ３８において、ステップＳ３５における比較結果の一致、すなわち、ＰＭＴから検出した編集スタジオコード（ＡＳＣ）と、メモリに格納した編集スタジオコード（ＡＳＣ）との一致、ステップＳ３６における比較結果の一致、すなわち、ＰＭＴから検出した情報記録媒体製造者コード（ＤＭＣ）と、メモリに格納した情報記録媒体製造者コード（ＤＭＣ）との一致、さらに、ステップＳ３７における規定時間内の電子透かし検出、照合のすべてを満足したか否かを判定する。

【０１４５】

ステップＳ３９において、ステップＳ３８の判定がＹｅｓであればコンテンツ再生を継続し、Ｎｏであれば、コンテンツ再生を停止する。

【０１４６】

図１３、図１４を参照してコンテンツ再生を実行するユーザデバイスとしての情報処理装置におけるコンテンツ再生処理手順の一連の処理について説明する。

【０１４７】

ステップＳ１０１において、情報処理装置（ユーザデバイス）は、情報記録媒体から暗号鍵情報および識別情報の読み取りを実行する。ステップＳ１０２において、読み取り情報および自デバイスに格納したデバイスキーに基づいてタイトルキー（Ｋｔ１，Ｋｔ２）を生成する。

【０１４８】

ステップＳ１０３において、情報記録媒体からディスクＩＤ（Ｓ，Ｓｉｇ）を読み取り、検証処理を実行する。検証が成立しない場合は、この時点でコンテンツ再生は停止する。検証が成立すると、ステップＳ１０５において、記録キーＫ１，Ｋ２を生成する。

【０１４９】

ステップＳ１０６において、第２タイトルキー（Ｋｔ２）に基づいて情報記録媒体から読み出した暗号化ＡＳＣ、暗号化ＤＭＣ、すなわち、ｅＫｔ２（ＡＳＣ）、ｅＫｔ２（ＤＭＣ）の復号処理を実行して、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）をメモリに格納する。

【０１５０】

ステップＳ１０７において、ブロックキーＫｂ１，Ｋｂ２を生成し、生成したブロックキーＫｂ１，Ｋｂ２に基づくコンテンツの復号、再生処理を開始する。

【０１５１】

ステップＳ１０８では、コンテンツ再生を実行しながらＰＭＴおよび電子透かしの検出処理を実行する。ステップＳ１０９においてＰＭＴから編集スタジオコード（ＡＳＣ）が検出されるとステップＳ１１０において検出した編集スタジオコード（ＡＳＣ）と、メモリに格納済みの編集スタジオコード（ＡＳＣ）との比較処理を実行し、一致しなかった場合は、ステップＳ１２１でコンテンツ再生を停止する。

【０１５２】

一致した場合は、さらに、ステップＳ１１１に進み、ＰＭＴから情報記録媒体製造者コード（ＤＭＣ）が検出されると、ステップＳ１１２において検出した情報記録媒体製造者コード（ＤＭＣ）と、メモリに格納済みの情報記録媒体製造者コード（ＤＭＣ）との比較処理を実行し、一致しなかった場合は、ステップＳ１２１でコンテンツ再生を停止する。

【０１５３】

一致した場合は、さらに、ステップＳ１１３に進み、電子透かし情報から編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）が検出されると、ステップＳ１１４において検出した編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ

）と、メモリに格納済みの編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）との比較処理を実行し、一致しなかった場合は、ステップＳ１２１でコンテンツ再生を停止する。

【０１５４】

ステップＳ１１５では、予め定めた時間内に、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）とのＰＭＴと電子透かし情報が検出されたか否かが判定され、検出されなかった場合は、ステップＳ１２１でコンテンツ再生を停止する。

【０１５５】

編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）とのＰＭＴ、電子透かし情報との検出処理は規定時間毎に繰り返し実行する。

【０１５６】

このようにして、暗号化コンテンツの復号およびコンテンツ再生制御が実行されることになる。なお、図１４のフローでは、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）とのＰＭＴ、電子透かし情報との検出処理を繰り返し実行する処理として説明したが、１つの編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）とのＰＭＴ、電子透かし情報との検出がなされ、両者がメモリ格納情報と一致した場合は、その後の電子透かし検出処理を実行しない構成としてもよい。

【０１５７】

上述したように、情報記録媒体に格納されたコンテンツは、シード情報（シード１）およびシード情報（シード２）によって生成されるブロック鍵Ｋｂ１，Ｋｂ２で暗号化され、シード情報（シード２）は、シード情報（シード１）を用いて生成される鍵、すなわちブロックキーＫｂ１によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード２）の解析、シード情報（シード２）を適用して生成するブロックキーＫｂ２の解析、ブロックキーＫｂ２によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

【０１５８】

さらに、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

【０１５９】

次に、図１５、図１６、図１７を参照してシード情報（シード１）と記録キーＫに基づいて生成するブロックキーＫｂ１によって暗号化する領域の例について説明する。図１５は、制御ブロックにシード情報（シード１）が格納され、シード情報（シード２）が、ユーザデータの１つのＴＳパケットに含まれる場合の例である。先に図１１を参照して説明した例では、シード情報（シード２）が、ユーザデータの先頭または２番目のＴＳパケット内に含まれる場合について説明したが、シード情報（シード２）は、先頭、または第２番目のＴＳパケット以外のユーザデータ部を構成する任意のＴＳパケット内に格納可能である。

【０１６０】

ユーザデータのいずれかのＴＳパケットにシード情報（シード２）を格納した場合、シード情報（シード１）と記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化する領域例として、例えば図１５（ａ）～（ｃ）の構成がある。（ａ）は、シード情報（シード２）のみをブロックキーＫｂ１によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報（シード２）と記録キーＫ２によって生成されるブロックキーＫｂ２によって暗号化したデータ領域とする。

【０１６１】
（ｂ）は、シード情報（シード２）を含むＴＳパケットの一部領域をブロックキーＫｂ１によって暗号化した例である。
【０１６２】
（ｃ）は、シード情報（シード２）を含む１つのＴＳパケットの全領域をブロックキーＫｂ１によって暗号化した例である。
【０１６３】
図１６に示す例は、シード情報（シード１）とシード情報（シード２）を同一のＴＳパケット内に格納した例を示している。シード情報（シード１）は非暗号化情報として格納される。シード情報（シード２）は、シード情報（シード１）と記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化され、シード情報（シード１）と同一のＴＳパケット内に格納される。
【０１６４】
（ｄ）は、シード情報（シード２）のみをブロックキーＫｂ１によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報（シード２）と記録キーＫ２によって生成されるブロックキーＫｂ２によって暗号化したデータ領域とする。
【０１６５】
（ｅ）は、シード情報（シード２）を含むＴＳパケットの一部領域をブロックキーＫｂ１によって暗号化した例である。（ｆ）は、シード情報（シード２）を含む１つのＴＳパケットの全領域をブロックキーＫｂ１によって暗号化した例である。
【０１６６】
図１７に示す例は、シード情報（シード１）とシード情報（シード２）を異なるＴＳパケット内に格納した例を示している。シード情報（シード１）は非暗号化情報として格納される。シード情報（シード２）は、シード情報（シード１）と記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化され、シード情報（シード１）と異なるＴＳパケット内に格納される。
【０１６７】
（ｇ）は、シード情報（シード２）のみをブロックキーＫｂ１によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報（シード２）と記録キーＫ２によって生成されるブロックキーＫｂ２によって暗号化したデータ領域とする。
【０１６８】
（ｈ）は、シード情報（シード２）を含むＴＳパケットの一部領域をブロックキーＫｂ１によって暗号化した例である。（ｉ）は、シード情報（シード２）を含む１つのＴＳパケットの全領域をブロックキーＫｂ１によって暗号化した例である。
【０１６９】
以上、図１５～図１７を参照して説明したように、シード情報（シード１）およびシード情報（シード２）の格納態様、および暗号化データ領域の設定態様は様々な設定が可能である。しかし、いずれの場合もシード情報（シード２）は、シード情報（シード１）を用いて生成される鍵、すなわちブロックキーＫｂ１によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード２）の解析、シード情報（シード２）を適用して生成するブロックキーＫｂ２の解析、ブロックキーＫｂ２によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。
【０１７０】
［情報記録媒体に対するデータ格納処理］
先に図２を参照して説明したように、暗号化コンテンツを格納した情報記録媒体は、コンテンツ編集エンティテイ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）３３０において編集され、その後、情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕ

ｒｅｒ）３５０において、ユーザに提供される媒体としてのＣＤ、ＤＶＤ等が大量に複製（レプリカ）されて、情報記録媒体１００が製造され、ユーザに提供される。

【０１７１】

このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ（ＴＣ：Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ）３００である。管理センタ（ＴＣ：Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ）３００は、コンテンツ編集エンティテイ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）３３０、および情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）３５０に対して様々な管理情報を提供し、コンテンツ編集エンティテイ（ＡＳ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ）３３０、および情報記録媒体製造エンティテイ（ＤＭ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）３５０は、管理センタ（ＴＣ：Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ）３００から受領した管理情報に基づいて、コンテンツ編集、暗号化、鍵情報の、生成、格納処理などを行う。

【０１７２】

管理センタ３００、コンテンツ編集エンティテイ３３０、および情報記録媒体製造エンティテイ３５０の実行する処理の詳細について、図１８以下を参照して説明する。

【０１７３】

図１８には、管理センタ３００、コンテンツ編集エンティテイ３３０、および情報記録媒体製造エンティテイ３５０の実行する処理を示している。

【０１７４】

管理センタ３００は、コンテンツ保持者からのコンテンツ５０１を保持し、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応してメディアキーＫｍ５０２、第２タイトルキーＫｔ２，５０３、第１タイトルキーＫｔ１，５０４、編集スタジオコード（ＡＳＣ）５０５、情報記録媒体製造者コード（ＤＭＣ）５０６、ディスク固有シードＳ５０７、製造を許容する情報記録媒体の数、量産発注枚数Ｎ５０８を設定する。

【０１７５】

管理センタ３００は、コンテンツ保持者からのコンテンツ５０１に対して、ステップＳ４１において、編集スタジオコード（ＡＳＣ）５０５、情報記録媒体製造者コード（ＤＭＣ）５０６を電子透かしとして埋め込む。

【０１７６】

ステップＳ４２では、ディスク固有シードＳ５０７に基づいて、ディスク固有キーＫｄ５１１を生成する。

【０１７７】

管理センタ３００は、電子透かしを埋め込んだコンテンツと、編集スタジオコード（ＡＳＣ）５０５、情報記録媒体製造者コード（ＤＭＣ）５０６、および、ディスク固有シードＳ５０７に基づいて生成したディスク固有キーＫｄ５１１をコンテンツ編集エンティテイ３３０に提供する。

【０１７８】

さらに、管理センタ３００は、ステップＳ４３において、メディアキーＫｍ５０２をコンテンツ再生権としてのライセンスを持つユーザデバイスのデバイスキーにおいてのみ取得可能な構成とした暗号鍵ブロックとしてのＥＫＢ５１２を生成する。

【０１７９】

ステップＳ４４では、メディアキーＫｍ５０２に基づいて第２タイトルキーＫｔ２，５０３を暗号化して暗号化第２タイトルキーｅＫｍ（Ｋｔ２）５１３を生成し、ステップＳ４５では、メディアキーＫｍ５０２に基づいて第１タイトルキーＫｔ１，５０４を暗号化して暗号化第１タイトルキーｅＫｍ（Ｋｔ１）５１４を生成する。

【０１８０】

さらに、ステップＳ４６において、編集スタジオコード（ＡＳＣ）５０５を第２タイトルキーＫｔ２，５０３で暗号化し、暗号化ＡＳＣであるｅＫｔ２（ＡＳＣ）５１５を生成し、ステップＳ４７において、情報記録媒体製造者コード（ＤＭＣ）５０６を第２タイトル

キーＫｔ２，５０３で暗号化し、暗号化ＤＭＣであるｅＫｔ２（ＤＭＣ）５１６を生成する。

【０１８１】

さらに、ディスク固有シードＳ５０７に対応して、製造を許容する情報記録媒体の数、量産発注枚数Ｎ５０８に基づくＮ個の（Ｓ，Ｓｉｇ）、すなわちＮ個の個別ディスクＩＤ５１７を生成する。

【０１８２】

ＥＫＢ５１２、暗号化第２タイトルキーｅＫｍ（Ｋｔ２）５１３、暗号化第１タイトルキーｅＫｍ（Ｋｔ１）５１４、暗号化ＡＳＣであるｅＫｔ２（ＡＳＣ）５１５、暗号化ＤＭＣであるｅＫｔ２（ＤＭＣ）５１６、Ｎ個の個別ディスクＩＤ５１７と第１タイトルキーＫｔ１は、管理センタ３００から、情報記録媒体製造エンティテイ３５０に提供される。

【０１８３】

次に、コンテンツ編集エンティテイ３３０の処理について説明する。コンテンツ編集エンティテイ３３０は、管理センタ３００から受領した電子透かし埋め込み済みのコンテンツの符号化、例えばＭＰＥＧ符号化処理をエンコーダ５３１において実行し、トラーンスポートストリームデータを生成し、さらに、管理センタ３００から受領した編集スタジオコード（ＡＳＣ）と、情報記録媒体製造者コード（ＤＭＣ）の埋め込み処理をＰＭＴ（Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）埋め込み部５３２において実行する。ＰＭＴは編集スタジオコード（ＡＳＣ）と、情報記録媒体製造者コード（ＤＭＣ）を含む情報であり、コンテンツ編集エンティテイ３３０においてコンテンツに対して埋め込まれる。

【０１８４】

次に暗号処理部５３３において暗号処理が実行される。コンテンツ編集エンティテイ３３０の暗号処理部５３３における処理の詳細について、図１９を参照して説明する。

【０１８５】

コンテンツ編集エンティテイ３３０は、ステップＳ５１において乱数に基づいて記録シード（ＲＥＣ　ＳＥＥＤ）を生成する。記録シード（ＲＥＣ　ＳＥＥＤ）は出力データとして、情報記録媒体製造エンティテイに渡されるデータである。さらに、ステップＳ５２において、管理センタ３００から受領したディスク固有キーＫｄと、記録シード（ＲＥＣ　ＳＥＥＤ）を適用した暗号処理により、記録キーＫ２を生成し、ステップＳ５３において、コンテンツ中から選択したシード情報（シード２）と記録キーＫ２とに基づいてブロックキーＫｂ２を生成（ステップＳ５４）し、ステップＳ５５において、ブロックキーＫｂ２に基づいて、コンテンツの暗号化処理を実行する。セレクタステップＳ５３ではシード２を選択するとともに、ステップＳ５５における暗号処理を実行するデータ部と、ステップＳ５５における暗号処理を実行しないデータ部が分離され、ステップＳ５６において暗号処理データと非暗号処理データとが再度結合されて出力データとして、記録シード（ＲＥＣ　ＳＥＥＤ）とともにディスクイメージデータとして情報記録媒体製造エンティテイに渡される。

【０１８６】

コンテンツ編集エンティテイ３３０の出力するデータは、図１９（ｂ）に示すように、シード情報（シード２）が平文データとして設定され、その他がシード２を適用して生成されるブロック鍵Ｋｂ２によって暗号化され、この暗号化データ中には、編集スタジオコード（ＡＳＣ）と、情報記録媒体製造者コード（ＤＭＣ）とを含むＰＭＴ（Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）が格納されている。

【０１８７】

次に、図１８に戻り、情報記録媒体製造エンティテイ３５０の処理について説明する。情報記録媒体製造エンティテイ３５０は、コンテンツ編集エンティテイ３５０からの受領コンテンツに対して、まず、暗号処理部５５１において暗号処理を実行する。

【０１８８】

情報記録媒体製造エンティテイ３５０の暗号処理部５５１において実行する暗号処理の詳細について図２０を参照して説明する。

【０１８９】
情報記録媒体製造エンティテイ３５０は、ステップＳ６１において乱数に基づいて物理インデックスを生成する。さらに、ステップＳ６２において、管理センタ３００から受領した第１タイトルキーＫｔ１と、物理インデックスを適用した暗号処理により、記録キーＫ１を生成し、ステップＳ６３において、コンテンツ中から選択したシード情報（シード１）と記録キーＫ１とに基づいてブロックキーＫｂ１を生成（ステップＳ６４）し、ステップＳ６５において、ブロックキーＫｂ１に基づいて、コンテンツ中のシード情報（シード２）を含むデータ領域の暗号化処理を実行する。セレクタステップＳ６３ではシード１を選択するとともに、ステップＳ６５における暗号処理を実行するデータ部と、ステップＳ６５における暗号処理を実行しないデータ部が分離され、ステップＳ６６において暗号処理データと非暗号処理データとが再度結合されて出力データとされる。

【０１９０】
情報記録媒体製造エンティテイ３５０の暗号処理部５５１の出力するデータは、図２０（ｂ）に示すように、シード情報（シード１）が平文データとして制御データ（ＵＣＤ：Ｕｓｅｒ　ｃｏｎｔｒｏＩ　Ｄａｔａ）中に設定され、シード２を含むデータ領域がシード１を適用して生成されるブロック鍵Ｋｂ１によって暗号化されたデータとなる。

【０１９１】
図１８に戻り、情報記録媒体製造エンティテイ３５０の処理について説明を続ける。情報記録媒体製造エンティテイ３５０の暗号処理部５５１の出力データは、フォーマット処理部５５２に入力され、管理センタ３００から受領するＥＫＢ５１２、暗号化第２タイトルキーｅＫｍ（Ｋｔ２）５１３、暗号化第１タイトルキーｅＫｍ（Ｋｔ１）５１４、暗号化ＡＳＣであるｅＫｔ２（ＡＳＣ）５１５、暗号化ＤＭＣであるｅＫｔ２（ＤＭＣ）５１６をディスクのリードイン領域（図１参照）に書き込む処理を実行する。その書き込み処理の際に、図２０（ａ）ステップＳ６１において生成された物理インデックスが同時に情報記録媒体に記録される。

【０１９２】
さらに、これらの情報を有する情報記録媒体（ディスク）のレプリカを複製製造部５５３において製造する。製造数は、管理センタ３００の設定した量産発注枚数Ｎに対応する数であり、各情報記録媒体毎に管理センタ３００から受領した異なるディスクＩＤが格納される。

【０１９３】
これらの全情報の格納処理がなされると、情報記録媒体１００が市場に流通し、ユーザに提供されユーザの情報処理装置において、前述した復号処理および再生制御処理に基づいてコンテンツ再生が実行される。情報記録媒体１００は、図１を参照して説明した各種の情報を格納し、ユーザの情報処理装置において、図８～図１４を参照して説明した復号、制御に基づく再生が実行される。

【０１９４】
［ディスクＩＤを用いない処理構成］
上述した実施例では、情報記録媒体に各媒体毎に異なるディスクＩＤを設定し、ユーザデバイス側でディスクＩＤを情報記録媒体から取得し、検証の後、ディスクＩＤの構成要素としてのディスク固有シードＳを適用してディスク固有キーＫｄを生成（図９ステップＳ１５）し、ディスク固有キーＫｄを適用したコンテンツ復号を実行する構成を説明した。

【０１９５】
しかし、情報記録媒体毎に異なるＩＤを記録する処理は手間がかかる処理であり、大量のディスクを量産する場合には、省略したい場合もある。以下、情報記録媒体毎に異なるディスクＩＤを用いない処理例について説明する。

【０１９６】
図２１に、管理センタ３００、コンテンツ編集エンティテイ３３０、および情報記録媒体製造エンティテイ３５０の実行するディスクＩＤを用いない処理例を示している。

【０１９７】

図２１において点線枠領域６００の構成が、先に図１８を参照して説明したディスクＩＤを適用した処理例と異なる部分である。なお、先に図１８を参照して説明したディスクＩＤ関連の処理、構成は、図２１には示されていない。

【０１９８】

管理センタ３００は、コンテンツ保持者からのコンテンツ５０１を保持し、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応してメディアキーＫｍ５０２、第２タイトルキーＫｔ２，５０３、第１タイトルキーＫｔ１，５０４、編集スタジオコード（ＡＳＣ）５０５、情報記録媒体製造者コード（ＤＭＣ）５０６、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応して設定される第３タイトルキーＫｔ３，６０１を設定する。

【０１９９】

本例においては、図１８を参照して説明したディスク固有シードＳ５０７、製造を許容する情報記録媒体の数、すなわち量産発注枚数Ｎ５０８が省略される。

【０２００】

管理センタ３００は、コンテンツ保持者からのコンテンツ５０１に対して、ステップＳ４１において、編集スタジオコード（ＡＳＣ）５０５、情報記録媒体製造者コード（ＤＭＣ）５０６を電子透かしとして埋め込む。

【０２０１】

管理センタ３００は、電子透かしを埋め込んだコンテンツと、編集スタジオコード（ＡＳＣ）５０５、情報記録媒体製造者コード（ＤＭＣ）５０６、および、ディスク固有キー（Ｄｉｓｃ　Ｕｎｉｑｕｅ　Ｋｅｙ）Ｋｄ，５１１をコンテンツ編集エンティテイ３３０に提供する。

【０２０２】

さらに、管理センタ３００は、ステップＳ４３において、メディアキーＫｍ５０２をコンテンツ再生権としてのライセンスを持つユーザデバイスのデバイスキーにおいてのみ取得可能な構成とした暗号鍵ブロックとしてのＥＫＢ５１２を生成する。

【０２０３】

ステップＳ４４では、メディアキーＫｍ５０２に基づいて第２タイトルキーＫｔ２，５０３を暗号化して暗号化第２タイトルキーｅＫｍ（Ｋｔ２）５１３を生成し、ステップＳ４５では、メディアキーＫｍ５０２に基づいて第１タイトルキーＫｔ１，５０４を暗号化して暗号化第１タイトルキーｅＫｍ（Ｋｔ１）５１４を生成する。

【０２０４】

さらに、ステップＳ４６において、編集スタジオコード（ＡＳＣ）５０５を第２タイトルキーＫｔ２，５０３で暗号化し、暗号化ＡＳＣであるｅＫｔ２（ＡＳＣ）５１５を生成し、ステップＳ４７において、情報記録媒体製造者コード（ＤＭＣ）５０６を第２タイトルキーＫｔ２，５０３で暗号化し、暗号化ＤＭＣであるｅＫｔ２（ＤＭＣ）５１６を生成する。

【０２０５】

さらに、ステップＳ７１において、第３タイトルキーＫｔ３，６０１をメディアキーＫｍ５０２に基づいて暗号化して暗号化第３タイトルキーｅＫｍ（Ｋｔ３）６０２を生成する。

【０２０６】

ＥＫＢ５１２、暗号化第２タイトルキーｅＫｍ（Ｋｔ２）５１３、暗号化第１タイトルキーｅＫｍ（Ｋｔ１）５１４、暗号化ＡＳＣであるｅＫｔ２（ＡＳＣ）５１５、暗号化ＤＭＣであるｅＫｔ２（ＤＭＣ）５１６、暗号化第３タイトルキーｅＫｍ（Ｋｔ３）６０２は、管理センタ３００から、情報記録媒体製造エンティテイ３５０に提供される。

【０２０７】

コンテンツ編集エンティテイ３３０の処理、情報記録媒体製造エンティテイ３５０の処理は、基本的に先に図１８～図２０を参照して説明した処理と同様である。ただし、情報記録媒体製造エンティテイ３５０のフォーマット処理部５５２は、情報記録媒体のリードイ

ン領域に書き込む処理を実行し、情報記録媒体製造エンティテイ３５０の複製製造部５５３は、ディスク毎のディスクＩＤの書き込み処理を実行しない。

【０２０８】

この結果として製造される情報記録媒体１００は、図２２に示すようなデータを格納することになる。

【０２０９】

図２２に示すように、情報記録媒体１００には、物理インデックス１０２、暗号化コンテンツ１０３、記録シード（ＲＥＣ　ＳＥＥＤ）１０４、暗号鍵情報１２０が格納される。暗号鍵情報１２０は、情報記録媒体１００のコンテンツ格納領域とは異なる特別のプログラムに基づいて読み取り可能なリードイン領域１１０に格納される。

【０２１０】

暗号鍵情報１２０には、暗号化第３タイトルキーｅＫｍ（Ｋｔ３）が含まれる。図１の構成と異なる点は、ディスクＩＤが格納されない点と、暗号鍵情報１２０に暗号化第３タイトルキーｅＫｍ（Ｋｔ３）６１１が追加された点である。

【０２１１】

この情報記録媒体を再生する情報処理装置（ユーザデバイス）の暗号処理手段の実行するコンテンツ復号処理について図２３を参照して説明する。

【０２１２】

図２３の処理中、先に図９を参照して説明したディスクＩＤを持つ情報記録媒体の再生処理と異なる点は、情報記録媒体１００が、暗号化第３タイトルキーｅＫｍ（Ｋｔ３）６１１を持つ点、ステップＳ８２のディスク固有キーＫｄの生成処理、ステップＳ８１の暗号化第３タイトルキーｅＫｍ（Ｋｔ３）６１１の復号処理である。

【０２１３】

本実施例においては、ディスク固有キーＫｄの生成処理をディスクＩＤから取得したディスク固有シードＳ（図９，ステップＳ１４参照）を適用しない。

【０２１４】

本実施例では、ステップＳ８１において、暗号化第３タイトルキーｅＫｍ（Ｋｔ３）６１１をメディアキーＫｍを用いて復号して、第３タイトルキーＫｔ３を取得し、取得した第３タイトルキーＫｔ３と、ステップＳ１２の復号処理で取得した第２タイトルキーＫｔ２に基づく暗号処理をステップＳ８２において実行してディスク固有キーＫｄの生成処理を実行する構成としている。

【０２１５】

以下の処理は、先に図９を参照して説明した処理と同様である。本処理例においては、ディスクＩＤを用いない構成であるので、情報記録媒体毎に異なるＩＤを記録する処理が不要となり、大量のディスクを量産する場合等、情報記録媒体製造エンティテイの処理が軽減される。

【０２１６】

本例においても、情報記録媒体に格納されたコンテンツは、シード情報（シード１）およびシード情報（シード２）によって生成されるブロック鍵Ｋｂ１，Ｋｂ２で暗号化され、シード情報（シード２）は、シード情報（シード１）を用いて生成される鍵、すなわちブロックキーＫｂ１によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード２）の解析、シード情報（シード２）を適用して生成するブロックキーＫｂ２の解析、ブロックキーＫｂ２によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

【０２１７】

さらに、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）の検出、照合一致を条件として再生処理を実行する構成としたので、不正なコードあるいは電子透かしを持たないコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となり、また不正な複製が製造され、流通した場合において、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を検出

することにより、情報の漏洩ルートを容易に追跡することが可能となる。

【０２１８】

［情報処理装置他のエンティテイ構成例］

次に、上述した各実施例において説明したユーザデバイスとしての情報処理装置、管理センタ、コンテンツ編集エンティテイ、情報記録媒体製造エンティテイ、各エンティテイが暗号処理、データ生成処理を実行するために適用する情報処理装置の構成例を図２４を参照して説明する。上述した各実施例において説明したユーザデバイスとしての情報処理装置、管理センタ、コンテンツ編集エンティテイ、情報記録媒体製造エンティテイ、各エンティテイが暗号処理、データ生成処理を実行するために適用する情報処理装置としては、例えばＰＣ、情報処理サーバ等の汎用的な情報処理装置が適用可能である。以下、図２４を参照して、上述した各エンティテイが暗号処理、データ生成処理を実行するために適用する情報処理装置の構成例について説明する。

【０２１９】

ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）７０１は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）７０２に記憶されている各種プログラム、あるいは、記憶部７０８に格納され、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）７０３にロードされたプログラムに従って各種処理を実行する。タイマ７００は計時処理を行ない、クロック情報をＣＰＵ７０１に供給する。

【０２２０】

ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）７０２は、ＣＰＵ７０１が使用するプログラムや演算用のパラメータ、固定データ等を格納する。ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）７０３は、ＣＰＵ７０１の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を格納する。これら各素子はバス７１１により相互に接続されている。

【０２２１】

暗号処理部７０４は、上述した各種の暗号処理、例えばＡＥＳ暗号化アルゴリズムを適用した暗号処理等を実行する。ＷＭ処理部７１３は、例えばスペクトラム拡散技術を用いて、データを不可視な情報としてビデオ信号へ埋め込む、あるいはデータを認識できない情報としてオーディオ信号へ埋め込む、などインフォメーションハイディング（Ｉｎｆｏｒｍａｔｉｏｎ　Ｈｉｄｉｎｇ）技術に基づく処理を実行する。

【０２２２】

入出力インタフェース７１２には、キーボード、マウス等の入力部７０６、ＣＲＴ、ＬＣＤ等のディスプレイ、スピーカ等からなる出力部７０７、ハードディスク等の記憶部７０８、通信部７０９が接続される。通信部７０９は、例えばインターネット等の通信網を介したデータ送受信により、たとえば各エンティテイ間の通信を行なう。

【０２２３】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２２４】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０２２５】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に予め記録しておくことができる。あるいは、プログラムはフレキシブル

ディスク、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ），ＭＯ（Ｍａｇｎｅｔｏ ｏｐｔｉｃａｌ）ディスク，ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ）、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０２２６】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０２２７】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０２２８】

【発明の効果】

以上、説明したように、本発明の構成によれば、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ＡＳＣ）と情報記録媒体製造者コード（ＤＭＣ）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

【０２２９】

さらに、本発明の構成によれば、情報記録媒体に格納されたコンテンツは、シード情報（シード１）およびシード情報（シード２）によって生成されるブロック鍵Ｋｂ１，Ｋｂ２で暗号化され、シード情報（シード２）は、シード情報（シード１）を用いて生成される鍵、すなわちブロックキーＫｂ１によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード２）の解析、シード情報（シード２）を適用して生成するブロックキーＫｂ２の解析、ブロックキーＫｂ２によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

【０２３０】

さらに、本発明の構成によれば、コンテンツ編集エンティティが、鍵生成情報としての記録シード（ＲＥＣ ＳＥＥＤ）を生成し、管理センタから受領する鍵情報、および鍵生成情報（第２シード）とに基づいて第２ブロックキーＫｂ２を生成し、第２ブロックキーＫｂ２に基づくコンテンツ暗号化を実行し、情報記録媒体製造エンティティが、鍵生成情報としての物理インデックスを生成し、管理センタから受領する鍵情報、および鍵生成情報（第１シード）に基づいてブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づく第２シードの暗号化を実行する構成とし、さらに、各エンティティのコード情報を情報記録媒体に格納する構成としたので、管理センタによって管理されたコンテンツ編集エンティティおよび情報記録媒体製造エンティティのみが正規な暗号化コンテンツを編集し、情報記録媒体を製造することが可能となり、情報記録媒体が不正に複製された場合には、コード検出による情報漏洩ルートの解析が可能となる。

【図面の簡単な説明】

【図１】情報記録媒体に格納されるデータ構成について説明する図である。

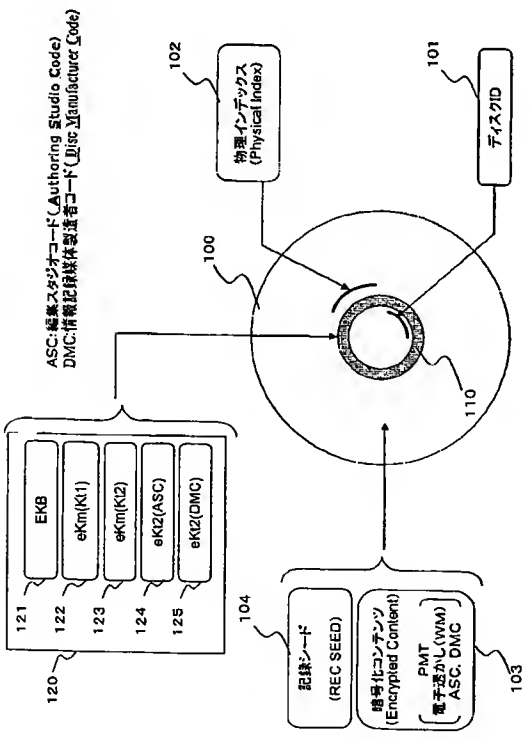
【図２】情報記録媒体に格納されるデータの管理、情報記録媒体の製造ルートについて説明する図である。

【図３】各種キー、データの暗号化処理、配布処理に適用される階層型木構造を説明する図である。
【図４】各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。
【図５】コンテンツ鍵の有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。
【図６】情報記録媒体に格納されるデータ構成について説明する図である。
【図７】情報処理装置の構成例について説明する図である。
【図８】情報処理装置において実行するコンテンツ復号、再生制御処理について説明する図である。
【図９】情報処理装置において実行するコンテンツ復号処理について説明する図である。
【図１０】ディスク固有キーの生成処理例について説明する図である。
【図１１】暗号化データの復号処理シーケンスを説明する図である。
【図１２】コンテンツの再生制御処理について説明する図である。
【図１３】コンテンツの復号処理および再生制御処理の手順について説明するフローチャートを示す図である。
【図１４】コンテンツの復号処理および再生制御処理の手順について説明するフローチャートを示す図である。
【図１５】シード情報の格納構成例について説明する図である。
【図１６】シード情報の格納構成例について説明する図である。
【図１７】シード情報の格納構成例について説明する図である。
【図１８】各エンティテイ毎の情報記録媒体に対して実行するデータ格納、暗号化処理を説明する図である。
【図１９】コンテンツ編集エンティテイの実行する暗号処理を説明する図である。
【図２０】情報記録媒体製造エンティテイの実行する暗号処理を説明する図である。
【図２１】ディスクＩＤを用いない処理例における各エンティテイ毎の情報記録媒体に対して実行するデータ格納、暗号化処理を説明する図である。
【図２２】ディスクＩＤを用いない処理例における情報記録媒体に格納されるデータ構成について説明する図である。
【図２３】ディスクＩＤを用いない処理例における情報処理装置において実行するコンテンツ復号処理について説明する図である。
【図２４】ユーザデバイス、各エンティテイにおいて適用する情報処理装置の構成例を示す図である。
【符号の説明】
１００　情報記録媒体
１０１　ディスクＩＤ
１０２　物理インデックス
１０３　暗号化コンテンツ
１０４　記録シード
１１０　リードイン領域
１２０　暗号鍵情報
１２１　ＥＫＢ
１２２　暗号化第１タイトルキーｅＫｍ（Ｋｔ１）
１２３　暗号化第２タイトルキーｅＫｍ（Ｋｔ２）
１２４　暗号化ＡＳＣ，ｅＫｔ２（ＡＳＣ）
１２５　暗号化ＤＭＣ：ｅＫｔ２（ＤＭＣ）
２００　情報処理装置
３００　管理センタ
３３０　コンテンツ編集エンティテイ
３５０　情報記録媒体製造エンティテイ

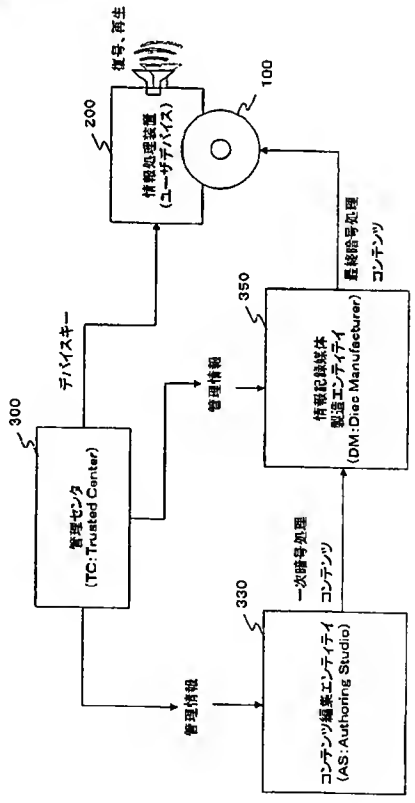
２１０　バス
２２０　入出力インタフェース
２３０　ＭＰＥＧコーデック
２４０　入出力インタフェース
２４１　Ａ／Ｄ，Ｄ／Ａコンバータ
２５０　暗号処理手段
２５５　再生制御処理手段
２６０　ＲＯＭ
２７０　ＲＡＭ
２８０　メモリ
２９０　記録媒体Ｉ／Ｆ
２９５　記録媒体
２９８　ＴＳ処理手段
４０１　ＥＫＢ
４０２　暗号化第２タイトルキーｅＫｍ（Ｋｔ２）
４０３　暗号化第１タイトルキーｅＫｍ（Ｋｔ１）
４０４　ディスクＩＤ
４０５　記録シード
４０６　物理インデックス
４０７　暗号化コンテンツ
４１０　デバイスキー
４１１　第２タイトルキーＫｔ２
４１２　コンテンツ
４２０　暗号処理単位
４２１　制御データ
４２２　先頭ＴＳパケット
４２３　後続ＴＳパケット
４２４　復号ＴＳパケット
４２５　復号ＴＳパケット群
４２６　復号ＴＳパケット
４３１　シード情報（シード１）
４３２　シード情報（シード２）
５０１　コンテンツ
５０２　メディアキー
５０３　第１タイトルキー
５０４　第２タイトルキー
５０５　コンテンツ編集エンティテイコード（ＡＳＣ：Ａｕｔｈｏｒｉｎｇ　Ｓｔｕｄｉｏ　Ｃｏｄｅ）
５０６　情報記録媒体製造者コード（ＤＭＣ：Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ　Ｃｏｄｅ）
５０７　ディスク固有シードＳ
５０８　量産発注コード
５１１　ディスク固有キーＫｄ
５１２　ＥＫＢ
５１３　暗号化第２タイトルキーｅＫｍ（Ｋｔ２）
５１４　暗号化第１タイトルキーｅＫｍ（Ｋｔ１）
５１５　暗号化ＡＳＣ，ｅＫｔ２（ＡＳＣ）
５１６　暗号化ＤＭＣ：ｅＫｔ２（ＤＭＣ）
５１７　個別ディスクＩＤ
５３１　エンコーダ

５３２　ＰＭＴ埋め込み部
５３３　暗号処理部
５５１　暗号処理部
５５２　フォーマット処理部
５５３　複製製造部
６０１　第３タイトルキーＫｔ３
６０２　暗号化第３タイトルキーｅＫｍ（Ｋｔ１）
６１１　暗号化第３タイトルキーｅＫｍ（Ｋｔ１）
７００　タイマ
７０１　ＣＰＵ（Ｃｅｎｔｒａｌ　ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）
７０２　ＲＯＭ（Ｒｅａｄ－Ｏｎｌｙ－Ｍｅｍｏｒｙ）
７０３　ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）
７０４　暗号処理部
７０６　入力部
７０７　出力部
７０８　記憶部
７０９　通信部
７１０　ドライブ
７１１　バス
７１２　入出力インタフェース
７１３　ＷＭ（Ｗａｔｅｒｍａｒｋ）処理部
７２１　リムーバブル記録媒体

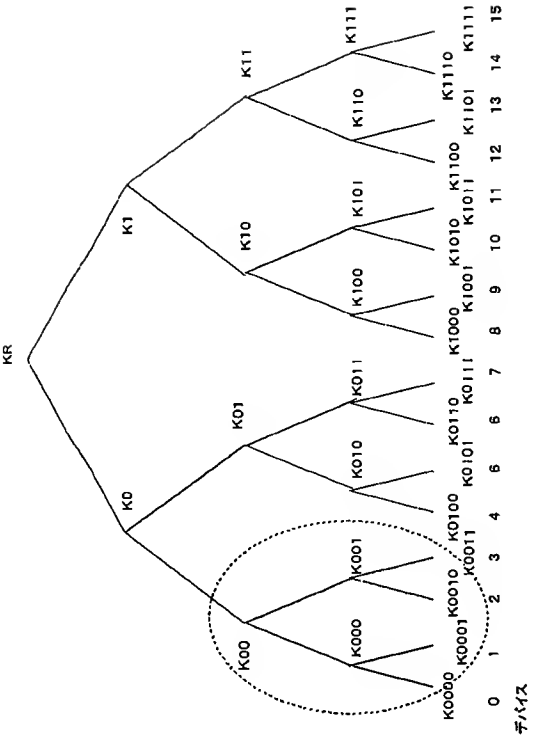
【図１】



【図２】



【図３】



【図４】

(A) 有効化キーブロック
(EKB:Enabling Key Block)例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

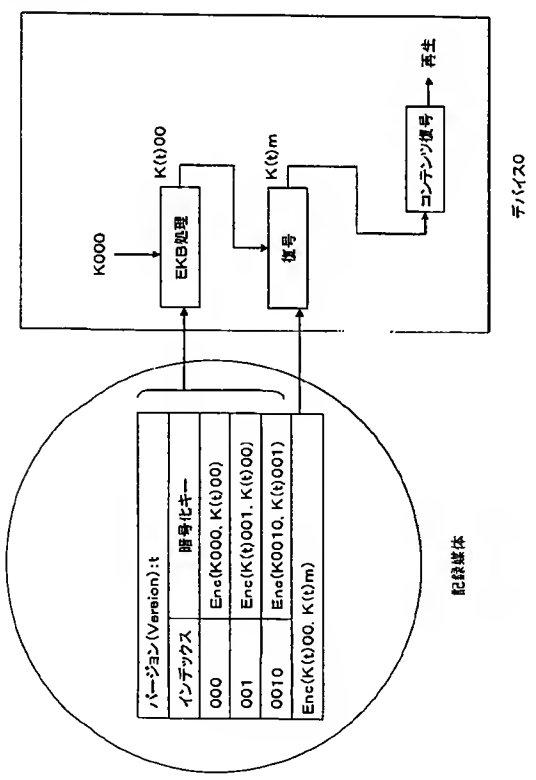
バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック
(EKB:Enabling Key Block) 例2

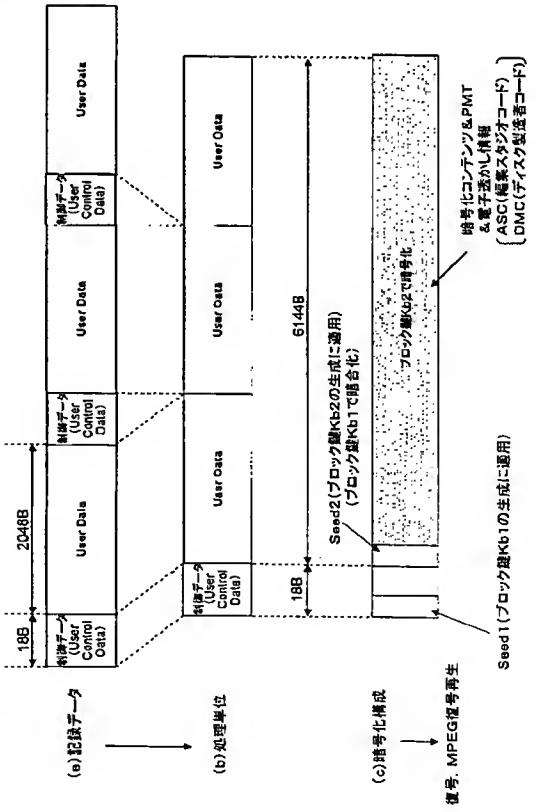
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

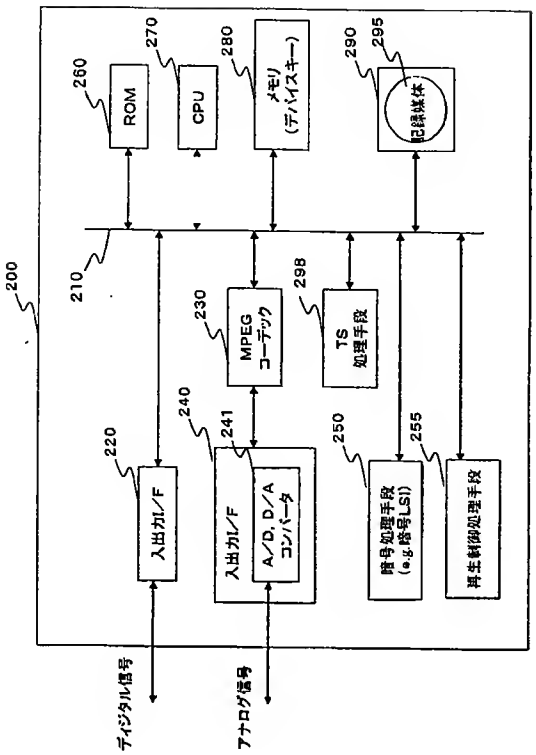
【図５】



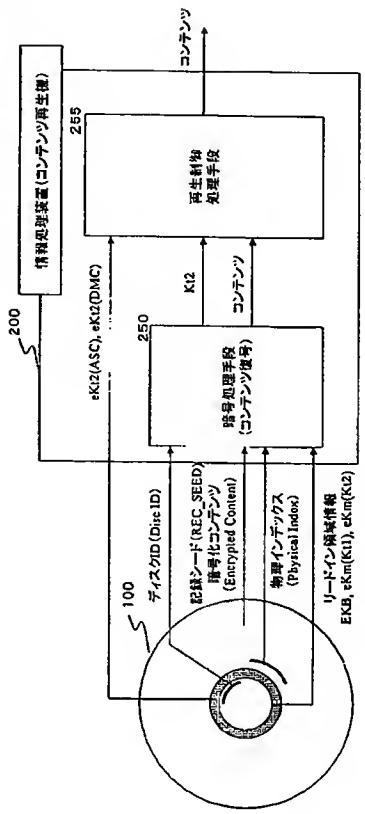
【図６】



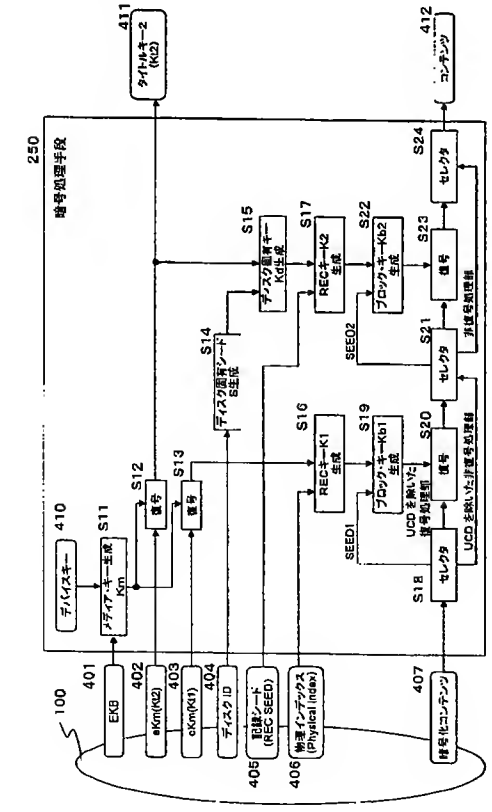
【図７】


200
210
260
ROM
270
CPU
280
メモリ
(デバイスキー)
290
295
記録媒体
220
入出力I/F
240
241
入出力I/F
A/D, D/A
コンバータ
230
MPEG
コーデック
298
TS
処理手段
250
暗号処理手段
(e.g.暗号LSI)
255
再生制御処理手段
ディジタル信号
アナログ信号

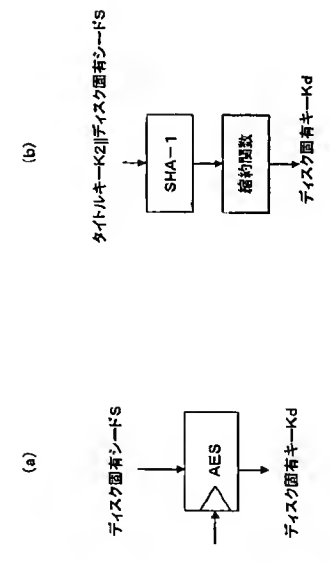
【図８】


200
情報処理装置(コンテンツ再生機)
コンテンツ
255
再生制御
処理手段
eK2(ASC), eK2(DMC)
250
暗号処理手段
(コンテンツ復号)
K12
コンテンツ
100
ディスクID(Disc ID)
記録シード(REC_SEED)
暗号化コンテンツ
(Encrypted Content)
物理インデックス
(Physical Index)
リードイン領域情報
EKB, eKm(K11), eKm(K12)

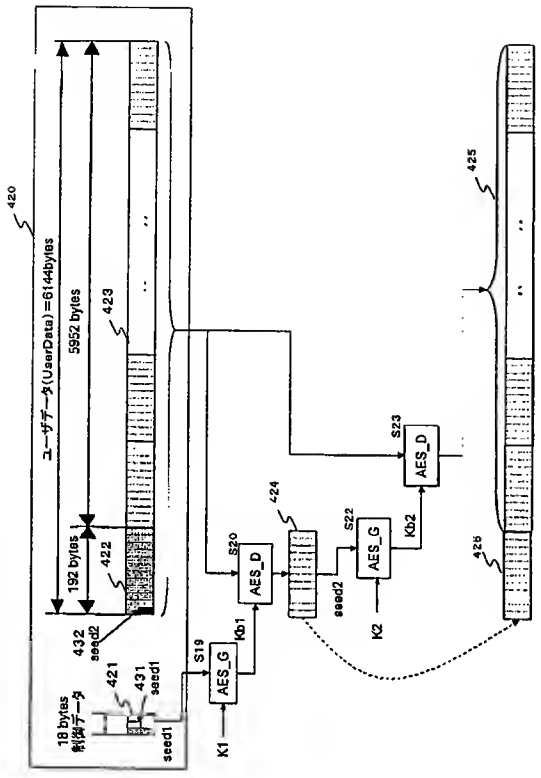
【図９】


100
401
EKB
402
eKm(K12)
403
eKm(K11)
404
ディスクID
405
記録シード
(REC_SEED)
406
物理インデックス
(Physical Index)
407
暗号化コンテンツ
250
暗号処理手段
410
デバイスキー
S11
S12
S13
S14
S15
S16
S17
S18
S19
S20
S21
S22
S23
S24
411
タイトルキー-2
(K12)
412
コンテンツ
SEED1
SEED2
UCDを用いた復号処理
UCDを用いた暗号処理

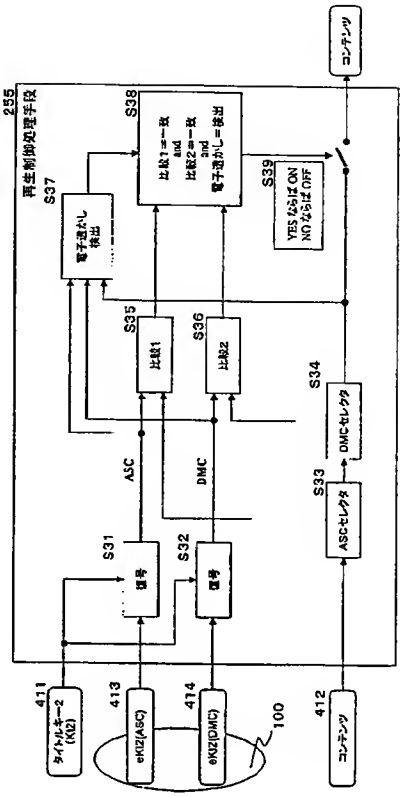
【図１０】


(a)
ディスク固有シードS
AES
タイトルキーK2
ディスク固有キーKd
(b)
タイトルキーK2||ディスク固有シードS
SHA-1
縮約関数
ディスク固有キーKd

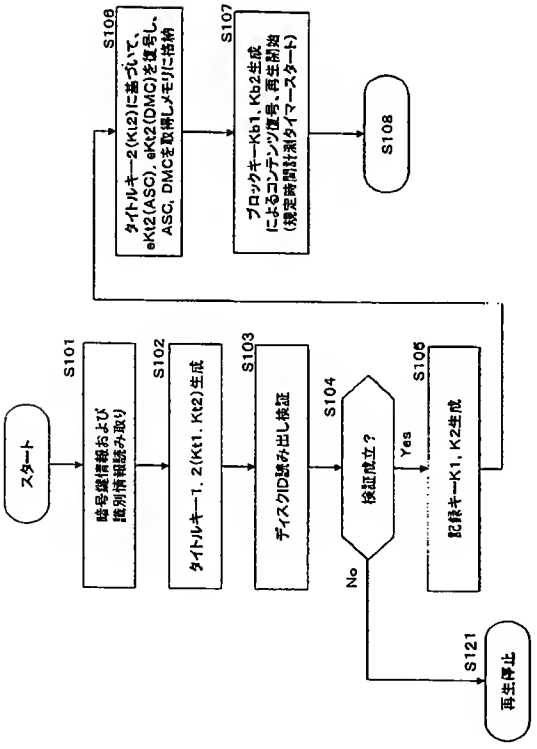
【図１１】



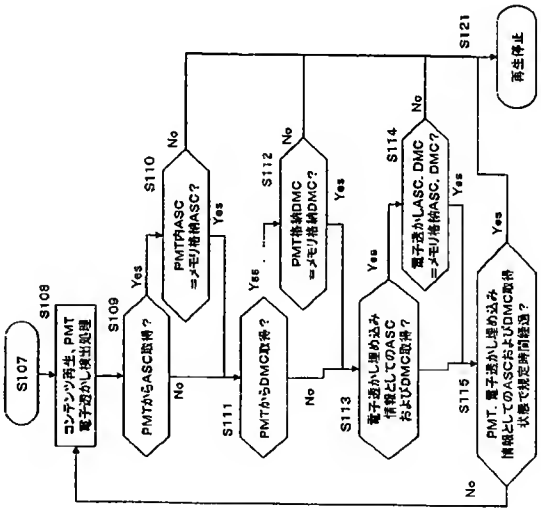
【図１２】



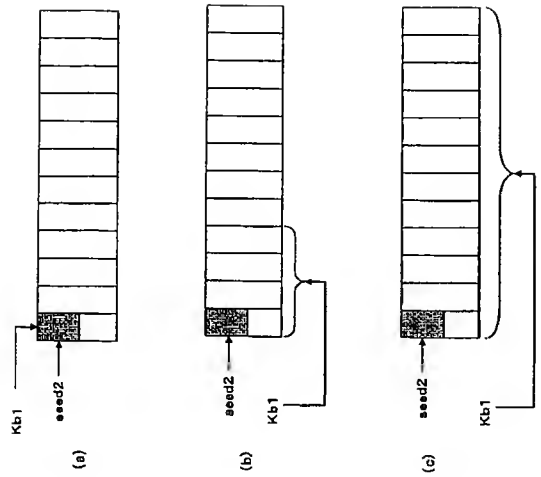
【図１３】



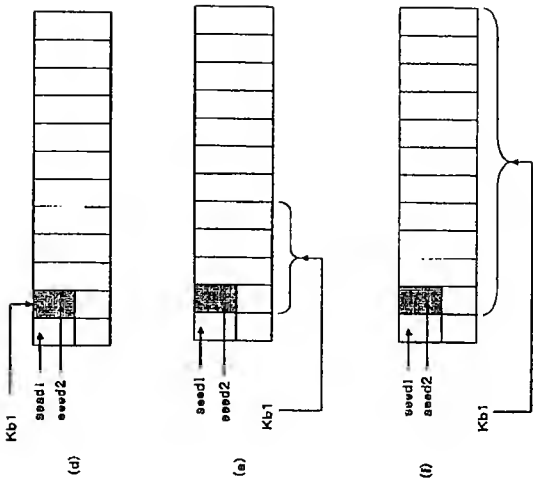
【図１４】



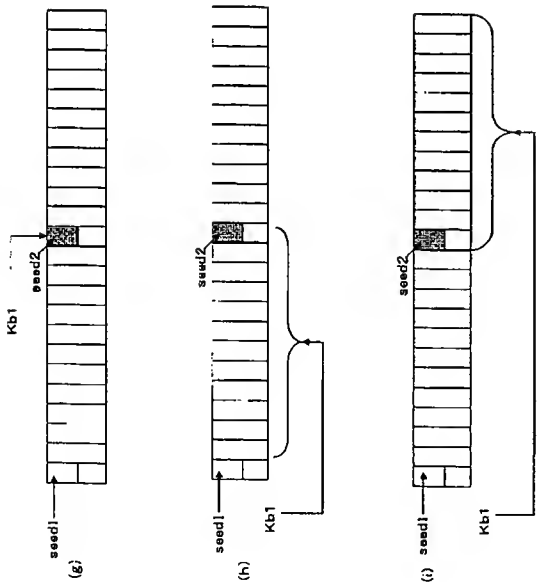
【図１５】



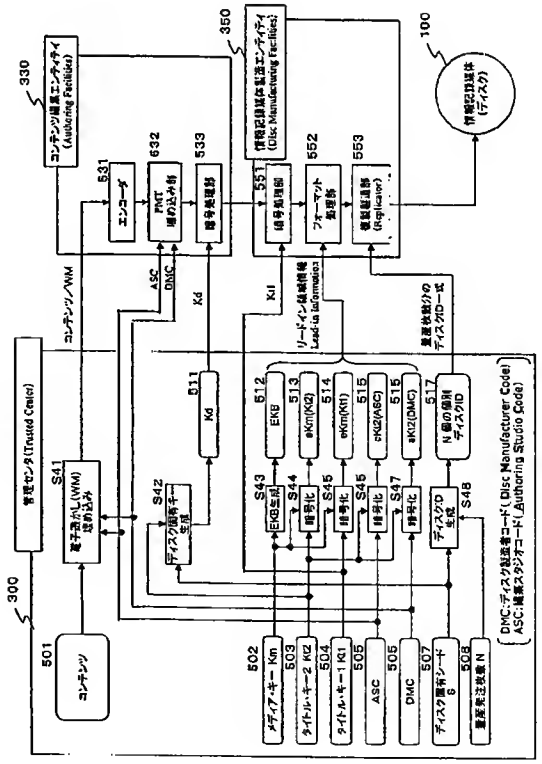
【図１６】



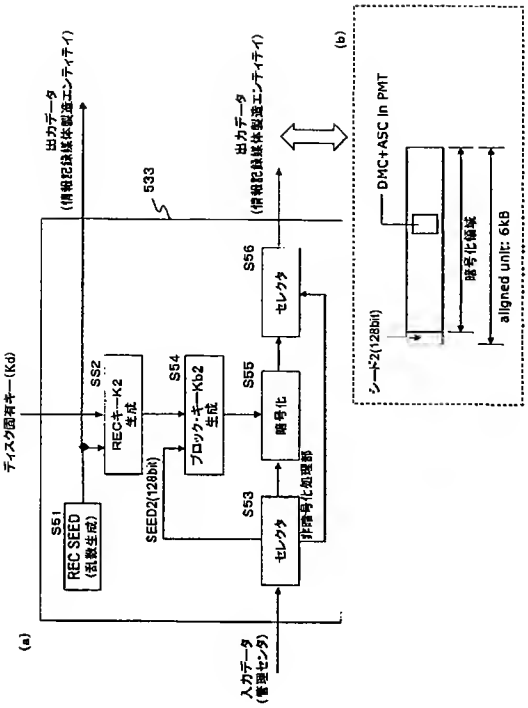
【図１７】



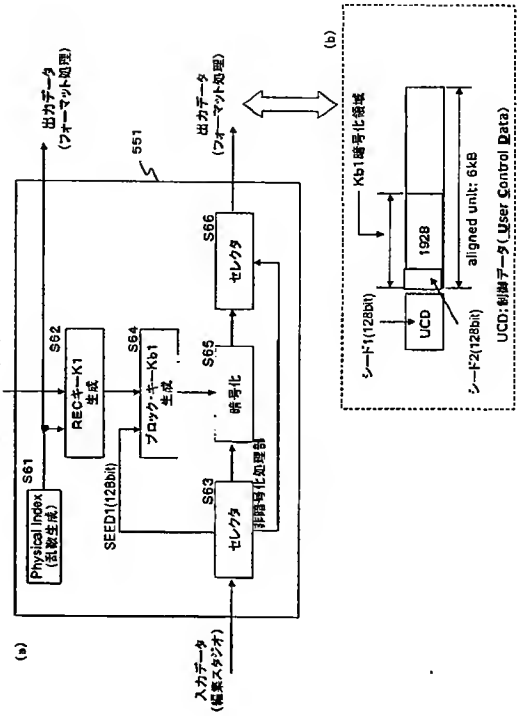
【図１８】



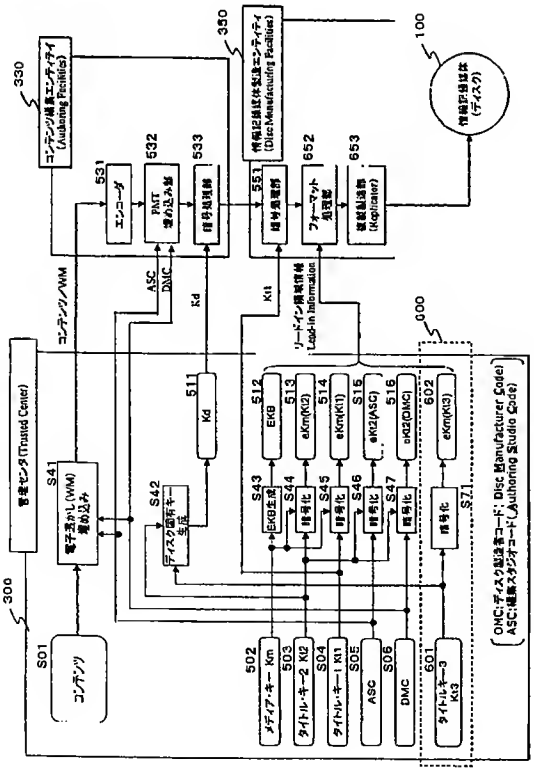
【図１９】



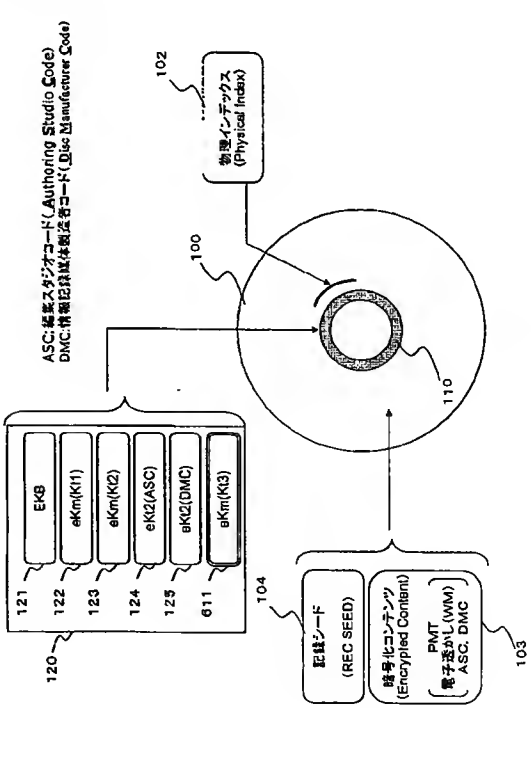
【図２０】



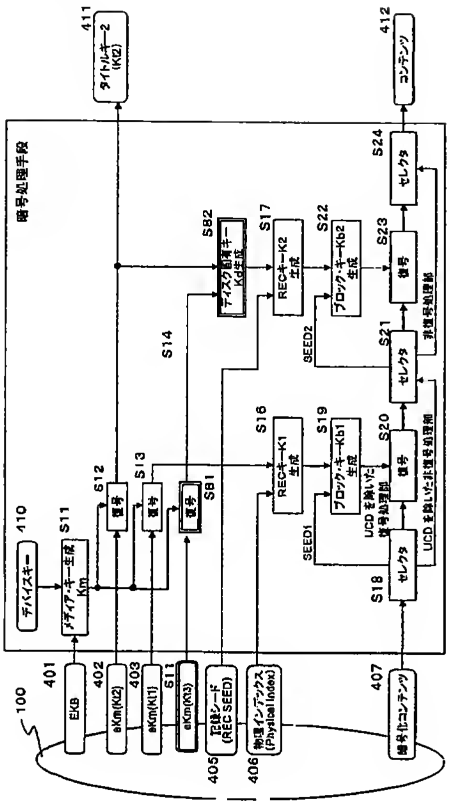
【図２１】



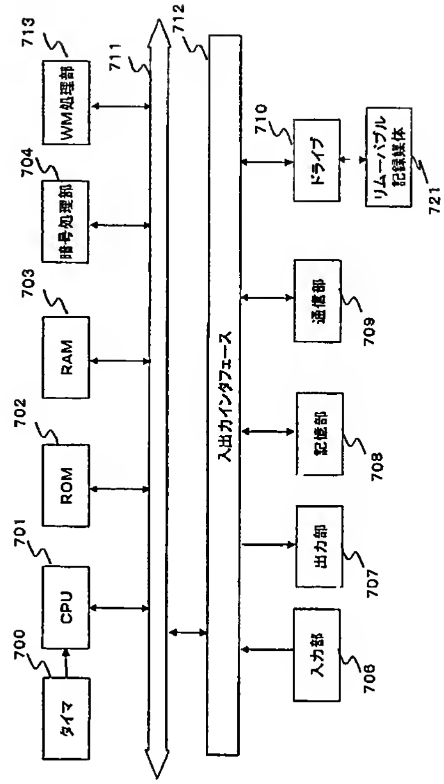
【図２２】



【図２３】


100
401
EKB
402
eKm(Kt2)
403
eKm(Kt1)
611
eKm(Kt3)
405
記録シード
(REC SEED)
406
物理インデックス
(Physical Index)
407
暗号化コンテンツ
250
暗号処理手段
410
デバイスキー
S11
メディア・キー生成
Km
S12
復号
S13
復号
SB1
復号
S14
SB2
ディスク固有キー
Kd生成
S16
RECキー-K1
生成
S17
RECキー-K2
生成
S19
ブロック・キー-Kb1
生成
S22
ブロック・キー-Kb2
生成
SEED1
SEED2
S18
セレクタ
S20
復号
UCDを除いた
復号処理部
UCDを除いた非復号処理部
S21
セレクタ
S23
復号
非復号処理部
S24
セレクタ
411
タイトルキー-2
(Kt2)
412
コンテンツ

【図２４】


700
タイマ
701
CPU
702
ROM
703
RAM
704
暗号処理部
713
WM処理部
711
712
入出力インタフェース
706
入力部
707
出力部
708
記憶部
709
通信部
710
ドライブ
721
リムーバブル
記録媒体

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	G11B 27/00	A	
	H04L 9/00	601A	
	H04L 9/00	601E	

(72)発明者 村松 克美
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72)発明者 高島 芳和
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72)発明者 米満 潤
東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B017 AA06 BA09 BB10 CA16
5D044 BC03 CC06 DE49 DE50 FG18 GK12 GK17 HL08
5D110 AA15 AA29 BB06 BB29 CA10 DA08 DB03 DE04
5J104 AA07 AA12 AA16 EA01 EA04 EA15 EA18 JA03 KA02 KA04
KA05 KA15 LA06 MA05 NA02 NA27 NA37 PA14